(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-112788
(P2004-112788A)
(43)公開日　平成16年4月8日(2004.4.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601B	5J104
H04L 9/32	H04L	9/00	601E	
	H04L	9/00	675B	

審査請求 未請求　請求項の数 24　OL　（全 94 頁）

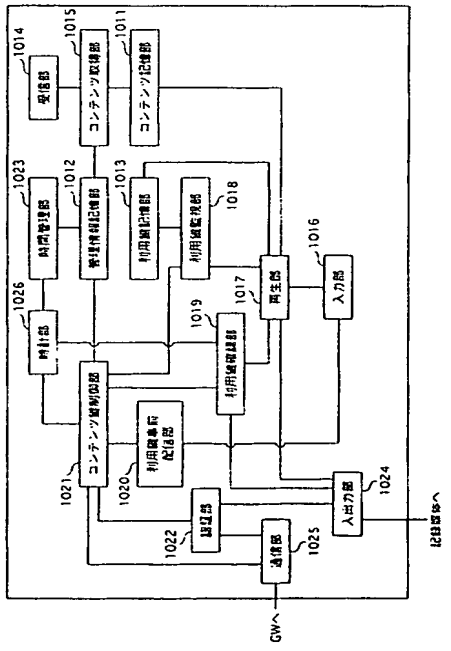
(21)出願番号　特願2003-305399(P2003-305399)
(22)出願日　平成15年8月28日(2003.8.28)
(31)優先権主張番号　特願2002-249242(P2002-249242)
(32)優先日　平成14年8月28日(2002.8.28)
(33)優先権主張国　日本国(JP)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(72)発明者　太田　雄策
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　山内　弘貴
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　宮▲ざき▼　雅也
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】鍵配信装置、端末装置、記録媒体及び鍵配信システム

(57)【要約】
【課題】　コンテンツが不正に使用されることを防止する鍵配信装置を提供することを目的とする。
【解決手段】　ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、前記端末装置から前記復号鍵の供給の要求を受け付け、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行い、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する。
【選択図】　図１７



【特許請求の範囲】
【請求項１】
ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、
前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、
供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断手段と、
供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、
前記供給判断手段は、少なくとも、可搬型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第１のタイプと判断する
ことを特徴とする鍵配信装置。
【請求項２】
前記ネットワークは、外部ネットワークに接続するホームネットワークであり、前記コンテンツは、前記ホームネットワーク外から受信され、前記鍵配信装置は、少なくともホームネットワークに接続される端末装置を、前記復号鍵の正当な供給先と判断する
ことを特徴とする請求項１に記載の鍵配信装置。
【請求項３】
前記鍵配信装置は、さらに、
前記第１のタイプの端末装置へ前記復号鍵と前記利用期限とを供給後、前記利用期限を記憶する配信鍵情報記憶手段と、
前記配信鍵情報記憶手段に記憶している前記利用期限が切れているか否かの判断を行う期限判断手段と、
前記利用期限が切れていると判断する場合には、前記管理数に１加算する時間管理手段と
を備えることを特徴とする請求項１に記載の鍵配信装置。
【請求項４】
前記鍵配信装置は、さらに、
前記復号鍵と前記利用期限とを供給すべき日時を示す供給日時と、供給先が第１のタイプの端末装置であることを示す識別情報とからなる組、又は前記復号鍵を供給すべき日時を示す供給日時と、供給先が第２のタイプの端末装置であることを示す識別情報とからなる組のうち少なくともどちらかを記憶する日時記憶手段と、
現在の日時が、前記供給日時記憶手段にて記憶されている供給日時に到達したか否かを判断する日時判断手段と、
前記日時判断手段が供給日時に到達したと判断する場合、前記識別情報に基いて、前記復号鍵と前記利用期限とを前記第１のタイプの端末装置へ供給、又は前記復号鍵を前記第２のタイプの端末装置へ供給する日時供給手段と
を備えることを特徴とする請求項３に記載の鍵配信装置。
【請求項５】
前記鍵配信装置は、さらに、
前記復号鍵を示す検索情報を前記第１タイプの端末装置及び前記第２のタイプの端末装置へ通知する検索要求手段と、
前記第１のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第１のタイプの端末装置より受け取り、前記第２のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第２のタイプの端末装置より受け取る所有情報受取手段と
を備えることを特徴とする請求項４に記載の鍵配信装置。

【請求項６】
前記鍵配信装置は、供給先が正当な供給先であるか否かの基準となる秘密情報を記憶しており、
前記供給判断手段は、供給先が、前記秘密情報を所有しているか否かの判断を行うサーバ認証手段を含み、
前記供給判断手段は、サーバ認証手段にて供給先が前記秘密情報を所有していると判断する場合に、正当な供給先と判断する
ことを特徴とする請求項５に記載の鍵配信装置。
【請求項７】
前記鍵配信手段は、前記復号鍵の管理数が、予め定められた基準値より大きいか否かを判断する残数判断手段を含み、
前記鍵配信手段は、前記残数判断手段にて、前記管理数が、前記基準値より大きいと判断する場合に、残数があると判断する
ことを特徴とする請求項６に記載の鍵配信装置。
【請求項８】
前記鍵供給手段は、さらに、
前記第１のタイプの端末装置へ前記復号鍵と前記利用期限とを供給する場合には、前記復号鍵と前記利用期限とを暗号化し、前記第２のタイプの端末装置へ前記復号鍵を供給する場合には、前記復号鍵を暗号化する暗号処理手段を備え、
前記鍵供給手段は、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを、前記暗号処理手段にて暗号化して、前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を、前記暗号処理手段にて暗号化して、前記端末装置へ供給する
ことを特徴とする請求項７に記載の鍵配信装置。
【請求項９】
前記鍵配信装置は、さらに、
前記第１のタイプの端末装置が接続された日時を示す履歴情報を記憶する履歴情報記憶手段と、
前記履歴情報を用いて、前記第１のタイプの端末装置が予め設定された接続期間内に接続がなされたか否かの判断を行う接続判断手段と、
前記接続期間内に接続がされていないと判断する場合には、前記管理数に１加算する接続管理手段とを
備えることを特徴とする請求項８に記載の鍵配信装置。
【請求項１０】
前記鍵配信装置は、さらに、
前記第１のタイプの端末装置が前記復号鍵を利用した回数を記憶する回数記憶手段と、
前記回数が、予め設定された利用回数に達したか否かの判断を行う回数判断手段と、
前記利用回数に達したと判断する場合には、前記管理数に１加算する接続管理手段とを
備えることを特徴とする請求項８に記載の鍵配信装置。
【請求項１１】
暗号化鍵にて暗号化されたコンテンツを復号する復号鍵を管理する鍵配信装置よりネットワークを介して前記復号鍵の供給を受ける端末装置であって、
前記鍵配信装置へ前記復号鍵を要求する要求手段と、
前記鍵配信装置にて前記復号鍵が供給可であると判断される場合に、前記復号鍵を、前記鍵配信装置より受け取る鍵受付手段と、
受け取った前記復号鍵を用いて、前記コンテンツの利用が終了したことを検知する検知手段と、
前記検知手段にて前記コンテンツの利用が終了したことを検知した場合に、前記復号鍵を消去し、前記復号鍵の利用が終了したことを示す利用終了情報を前記鍵配信装置へ通知

する終了通知手段と
を備えることを特徴とする端末装置。
【請求項１２】
前記端末装置は、さらに、
前記鍵受付手段にて受け取った復号鍵を用いて、前記暗号化されたコンテンツを復号して、コンテンツを生成し、生成したコンテンツを利用する利用手段を備え、
前記検知手段は、前記利用手段による前記コンテンツの利用終了が終了したことを検知する
ことを特徴とする請求項１１に記載の端末装置。
【請求項１３】
前記鍵受付手段は、さらに、
前記鍵配信装置より前記復号鍵を受け取る場合に、暗号化された復号鍵を受け取り、受け取った暗号化された復号鍵を復号して、前記復号鍵を生成する復号処理手段を備えることを特徴とする請求項１２に記載の端末装置。
【請求項１４】
前記端末装置は、コンテンツの利用期限の管理を行う端末装置であって、
前記鍵受付手段は、さらに、前記復号鍵の利用期限を受け取り、
前記端末装置は、さらに、前記鍵受付手段にて受け取った前記期間情報にて示される前記利用期限が期限内であるか否かの判断を行う期限判断手段を備え、
前記検知手段は、前記期限判断手段にて、前記復号鍵の利用期限が過ぎたと判断する場合に、前記コンテンツの利用が終了したと検知する
ことを特徴とする請求項１１に記載の端末装置。
【請求項１５】
前記鍵受付手段は、さらに、
前記鍵配信装置より前記復号鍵と前記利用期限を受け取る場合に、暗号化された復号鍵と利用期限とを受け取り、受け取った暗号化された復号鍵と利用期限とを復号して、前記復号鍵と前記利用期限とを生成する復号処理手段を
備えることを特徴とする請求項１２に記載の端末装置。
【請求項１６】
前記端末装置は、さらに、
前記鍵配信装置より前記復号鍵を示す検索情報を受け取り、受け取った前記検索情報を用いて、前記復号鍵を所有しているか否かの判断を行う所有判断手段と、
前記所有判断手段にて、前記復号鍵を所有していると判断する場合には、前記復号鍵を所有する旨の情報を、前記鍵配信装置へ通知する所有通知手段と
を備えることを特徴とする請求項１１に記載の端末装置。
【請求項１７】
暗号化鍵にて暗号化されたコンテンツを復号する復号鍵を管理する鍵配信装置より前記復号鍵の供給を受ける可搬型の記録媒体であって、
前記鍵配信装置にて前記復号鍵が供給可であると判断される場合に、前記復号鍵と前記復号鍵の利用期限とを、前記鍵配信装置より受け取る鍵受付手段と、
受け取った前記復号鍵と前記利用期限とを記憶する鍵情報記憶手段と
を備えることを特徴とする記録媒体。
【請求項１８】
前記鍵受付手段は、さらに、
前記鍵配信装置より前記復号鍵と前記利用期限を受け取る場合に、暗号化された復号鍵と利用期限とを受け取り、受け取った暗号化された復号鍵と利用期限とを復号して、前記復号鍵と前記利用期限とを生成する復号処理手段を
備えることを特徴とする請求項１７に記載の記録媒体。
【請求項１９】
前記記録媒体は、さらに、

前記利用期限が切れているか否かの判断を行う期限判断手段と、

期限判断手段にて利用期限が切れていると判断する場合に、前記復号鍵と利用期限とを消去する消去手段と

を備えることを特徴とする請求項１７に記載の記録媒体。

【請求項２０】

前記記録媒体は、さらに、

前記鍵配信装置より、前記復号鍵を示す鍵検索情報を受け取り、受け取った前記鍵検索情報を用いて、前記復号鍵を所有しているか否かの判断を行う所有判断手段と、

前記所有判断手段にて、前記復号鍵を所有していると判断する場合には、前記復号鍵を所有する旨の情報を、前記鍵配信装置へ通知する所有通知手段と

を備えることを特徴とする請求項１７に記載の記録媒体。

【請求項２１】

ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置と、コンテンツの利用期限の管理を行う第１タイプの端末装置と、コンテンツの利用期限の管理を行わない第２タイプの端末装置とからなる鍵配信システムであって、

前記鍵配信装置は、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第1タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断手段と、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、前記供給判断手段は、少なくとも、可搬型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第1のタイプと判断し、

前記第１のタイプの端末装置は、

前記鍵配信装置より前記復号鍵と前記利用期限とを受け取り、受け取った前記復号鍵と前記利用期限とを記憶し、

前記第２のタイプの端末装置は、

前記鍵配信装置より前記復号鍵を受け取り、受け取った前記復号鍵を用いて、コンテンツを利用する

ことを特徴とする鍵配信システム。

【請求項２２】

ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置に用いられる鍵供給方法であって、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付ステップと、

供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断ステップと、

供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給ステップと

を含むことを特徴とする鍵供給方法。

【請求項２３】

ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置に用いられる鍵供給プログラムであって、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付ステップと、
供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断ステップと、
供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給ステップと
を含むことを特徴とする鍵供給プログラム。
【請求項２４】
ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置に用いられる鍵供給プログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、
前記鍵供給プログラムは、
前記端末装置から前記復号鍵の供給の要求を受け付ける受付ステップと、
供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断ステップと、
供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給ステップと
を含むことを特徴とするプログラム記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化されたコンテンツを復号する鍵を配信する技術に関する。
【背景技術】
【０００２】
近年、映画、音楽、ゲームプログラム等のデジタル化されたコンテンツにおける著作権の保護が求められており、コンテンツの管理が重要となってきている。
特許文献１において、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理に有効な技術が開示されている。この方法では、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に複製コンテンツを記録する記録装置と、該記録媒体との間の相互認証を行い、該記録装置は、認証が成功すると該記録媒体へ複製コンテンツを複製若しくは、削除することによりコンテンツ利用の管理を行っている。
【特許文献１】特開２０００－３５７２１３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、上記に示した方法では、記録装置は、ネットワークに接続された装置に記録された複製コンテンツ利用の管理を常に行うことはできるが、記録媒体に記録された複製コンテンツ利用の管理を行うことができるのは、前記記録媒体と接続された場合のみである。そのため、例えば、前記記録媒体が、第三者によって、前記記録媒体に記録されている複製コンテンツが不正に使用される可能性がある。
【０００４】
そこで、本発明では、上記問題点を解決するために、コンテンツが不正に使用されることを防止する鍵配信装置、端末装置、記録媒体、鍵配信システム、鍵配信方法、プログラムを提供することを目的とする。
【課題を解決するための手段】

【０００５】
上記目的を達成するために、本発明は、ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断手段と、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、前記供給判断手段は、少なくとも、可搬型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第１のタイプと判断することを特徴とする。

【発明の効果】

【０００６】
本発明は、ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行う供給判断手段と、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、前記供給判断手段は、少なくとも、可搬型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第１のタイプと判断することを特徴とする。

【０００７】
この構成によると、鍵配信装置は、復号鍵の供給先が正当な供給先であれば、供給先が、第１のタイプの端末装置であるか又は第２のタイプの端末装置であるかの判断を行い、供給先が第１のタイプの端末装置である場合には、利用期限を付加した復号鍵を供給し、供給先が第２のタイプの端末装置である場合には、復号鍵を供給する。これにより、第１のタイプの端末装置には、利用期限を付加した復号鍵が供給されるため、第1のタイプの端末装置は、供給された利用期限と復号鍵とを使用することにより、コンテンツ利用の管理が可能となり、コンテンツの不正使用を防止することができる。

【０００８】
ここで、前記ネットワークは、外部ネットワークに接続するホームネットワークであり、前記コンテンツは、前記ホームネットワーク外から受信され、前記鍵配信装置は、少なくともホームネットワークに接続される端末装置を、前記復号鍵の正当な供給先と判断するとしてもよい。

この構成によると、鍵配信装置は、ホームネットワークに接続される端末装置を正当な供給先と判断し、復号鍵を供給することができる。

【０００９】
ここで、前記鍵配信装置は、さらに、前記第１のタイプの端末装置へ前記復号鍵と前記利用期限とを供給後、前記利用期限を記憶する配信鍵情報記憶手段と、前記配信鍵情報記憶手段に記憶している前記利用期限が切れているか否かの判断を行う期限判断手段と、前記利用期限が切れていると判断する場合には、前記管理数に１加算する時間管理手段とを備えるとしてもよい。

【００１０】
この構成によると、前記第１のタイプの端末装置へ供給した復号鍵の利用期限を管理することにより、管理数の管理ができる。

ここで、前記鍵配信装置は、さらに、前記復号鍵と前記利用期限とを供給すべき日時を示す供給日時と、供給先が第１のタイプの端末装置であることを示す識別情報とからなる組、又は前記復号鍵を供給すべき日時を示す供給日時と、供給先が第２のタイプの端末装置であることを示す識別情報とからなる組のうち少なくともどちらかを記憶する日時記憶手段と、現在の日時が、前記供給日時記憶手段にて記憶されている供給日時に到達したか否かを判断する日時判断手段と、前記日時判断手段が供給日時に到達したと判断する場合、前記識別情報に基いて、前記復号鍵と前記利用期限とを前記第１のタイプの端末装置へ供給、又は前記復号鍵を前記第２のタイプの端末装置へ供給する日時供給手段とを備えるとしてもよい。

【００１１】

この構成によると、供給日時記憶手段にて記憶されている供給日時となった場合に、復号鍵の供給を行うことができる。

ここで、前記鍵配信装置は、さらに、前記復号鍵を示す検索情報を前記第１タイプの端末装置及び前記第２のタイプの端末装置へ通知する検索要求手段と、前記第１のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第１のタイプの端末装置より受け取り、前記第２のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第２のタイプの端末装置より受け取る所有情報受取手段とを備えるとしてもよい。

【００１２】

この構成によると、鍵配信装置は、鍵検索情報を第１のタイプの端末装置及び第２のタイプの端末装置へ送信し、復号鍵を所有する旨の情報を受信することにより、復号鍵の供給先を検索することができる。

ここで、前記鍵配信装置は、供給先が正当な供給先であるか否かの基準となる秘密情報を記憶しており、前記供給判断手段は、供給先が、前記秘密情報を所有しているか否かの判断を行うサーバ認証手段を含み、前記供給判断手段は、サーバ認証手段にて供給先が前記秘密情報を所有していると判断する場合に、正当な供給先と判断するとしてもよい。

【００１３】

この構成によると、秘密情報を用いて、正当な供給先であるか否かの判断が可能となる。

ここで、前記鍵配信手段は、前記復号鍵の管理数が、予め定められた基準値より大きいか否かを判断する残数判断手段を含み、前記鍵配信手段は、前記残数判断手段にて、前記管理数が、前記基準値より大きいと判断する場合に、残数があると判断するとしてもよい。

【００１４】

この構成によると、管理数と基準値とを用いて、残数の有無の判断を行うことが可能となる。

ここで、前記鍵供給手段は、さらに、前記第１のタイプの端末装置へ前記復号鍵と前記利用期限とを供給する場合には、前記復号鍵と前記利用期限とを暗号化し、前記第２のタイプの端末装置へ前記復号鍵を供給する場合には、前記復号鍵を暗号化する暗号処理手段を備え、前記鍵供給手段は、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを、前記暗号処理手段にて暗号化して、前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を、前記暗号処理手段にて暗号化して、前記端末装置へ供給するとしてもよい。

【００１５】

この構成によると、復号鍵を供給する場合に暗号化することにより、安全に復号鍵の供給ができる。

ここで、前記鍵配信装置は、さらに、前記第１のタイプの端末装置が接続された日時を示す履歴情報を記憶する履歴情報記憶手段と、前記履歴情報を用いて、前記第１のタイプの端末装置が予め設定された接続期間内に接続がなされたか否かの判断を行う接続判断手

段と、前記接続期間内に接続がされていないと判断する場合には、前記管理数に１加算する接続管理手段とを備えるとしてもよい。

【００１６】

この構成によると、復号鍵を記憶している第１のタイプの端末装置が、予め設定された期間内に鍵配信装置と接続がなされたか否かを判断することにより、管理数の管理が可能となる。

ここで、前記鍵配信装置は、さらに、前記第１のタイプの端末装置が前記復号鍵を利用した回数を記憶する回数記憶手段と、前記回数が、予め設定された利用回数に達したか否かの判断を行う回数判断手段と、前記利用回数に達したと判断する場合には、前記管理数に１加算する接続管理手段とを備えるとしてもよい。

【００１７】

この構成によると、第１のタイプの端末装置へ供給した復号鍵を利用した回数が、予め記憶している利用回数に達したか否かを判断することにより、管理数の管理が可能となる。

また、本発明は、暗号化鍵にて暗号化されたコンテンツを復号する復号鍵を管理する鍵配信装置より前記復号鍵の供給を受ける可搬型の記録媒体であって、前記鍵配信装置にて前記復号鍵が供給可であると判断される場合に、前記復号鍵と前記復号鍵の利用期限とを、前記鍵配信装置より受け取る鍵受付手段と、受け取った前記復号鍵と前記利用期限とを記憶する鍵情報記憶手段とを備える。

【００１８】

この構成によると、記録媒体は、受け取った期限付復号鍵を用いて、復号鍵と利用期限とを生成し、生成した復号鍵と利用期限とを記憶することができる。

ここで、前記記録媒体は、さらに、前記利用期限が切れているか否かの判断を行う期限判断手段と、期限判断手段にて利用期限が切れていると判断する場合に、前記復号鍵と利用期限とを消去する消去手段とを備えるとしてもよい。

【００１９】

この構成によると、前記利用期限が過ぎている場合には、記憶している復号鍵と利用期限とを消去する。これにより、利用期限が過ぎている復号鍵の利用を防止することができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

１．　グループ形成管理システム１の構成

グループ形成管理システム１は図１に示すように、ＡＤ内サーバ１００、再生装置２００、車載機器３００、ＩＣカード４００及びＤＶＤ５００から構成される。

ＡＤ内サーバ１００及びモニタ２５１とスピーカ２５２とが接続されている再生装置２００は、ユーザ宅内に設置されており、オンラインで接続されている。車載機器３００は、ユーザが所有する車両に搭載されている。ＩＣカード４００及びＤＶＤ５００は、ＡＤ内サーバ１００及び車載機器３００に接続可能である。ＩＣカード４００はＡＤ内サーバ１００に付属しており、ＡＤ内サーバ１００は、ＩＣカード４００が接続されている場合のみ、動作する。

【００２１】

グループ形成管理システム１は、ＡＤ内サーバ１００が、コンテンツの利用が許可される範囲であるＡＤ（Ａｕｔｈｏｒｉｚｅｄ　Ｄｏｍａｉｎ）を管理するシステムである。

ＡＤ内サーバ１００は、クライアント機器の登録を受け付けて管理し、ＡＤ内サーバ１００及び登録されたクライアント機器は、ＡＤ内サーバ１００により生成された共通秘密情報（以下ＣＳＩ：Ｃｏｍｍｏｎ　Ｓｅｃｒｅｔ　Ｉｎｆｏｒｍａｔｉｏｎ）を共有する。同一ＡＤ内の機器間では、共有したＣＳＩを用いてお互いを認証し、認証に成功した場合にコンテンツの送受信やコピーを行う。前記ＣＳＩを持たない機器は、コンテンツの送受信やコピーを行うことは出来ない。

【００２２】
再生装置２００は、ＡＤ内サーバ１００と接続されているので、認証を行い、クライアント機器として登録することが出来る。また、車載機器３００は、ＡＤ内サーバ１００と接続されていないが、ＩＣカード４００にＣＳＩを記憶させ、ＩＣカード４００から車載機器３００にＣＳＩを通知することによってクライアント機器として登録することが出来る。

１．１　ＡＤ内サーバ１００の構成

ＡＤ内サーバ１００は図２に示すように、制御部１０１、秘密鍵格納部１０２、公開鍵証明書格納部１０３、ＣＲＬ格納部１０４、公開鍵暗号処理部１０５、登録情報記憶部１０６、ＣＳＩ生成部１０７、ＣＳＩ格納部１０８、コンテンツ格納部１０９、暗号化部１１０、ＩＤ格納部１１１、ドライブ部１１２、入力部１１３、表示部１１４、入出力部１１５、入出力部１１６、復号部１１７及び暗号化部１１９から構成される。

【００２３】
ＡＤ内サーバ１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、ＡＤ内サーバ１００は、その機能を達成する。

【００２４】
ＡＤ内サーバ１００は、機器の登録、ＣＳＩの移動及び脱退の管理、コンテンツの配送及びコンテンツのコピーの処理を行う。

以下、各構成について説明する。

（１）入出力部１１５，１１６、ドライブ部１１２

入出力部１１５は、再生装置２００とデータの送受信を行う。入出力部１１６は、ＩＣカード４００が接続されたことを検出すると、制御部１０１に検出を出力する。また、ＩＣカード４００とデータの送受信を行う。ドライブ部１１２は、ＤＶＤ５００へデータの書き込み、読み出しを行う。

（２）秘密鍵格納部１０２、公開鍵証明書格納部１０３、ＣＲＬ格納部１０４、コンテンツ格納部１０９、ＩＤ格納部１１１、コンテンツ鍵格納部１１８

ＩＤ格納部１１１は、ＡＤ内サーバ１００に固有のＩＤであるＩＤ＿１を記憶している。

【００２５】
公開鍵証明書格納部１０３は、公開鍵証明書Ｃｅｒｔ＿１を格納する。

公開鍵証明書Ｃｅｒｔ＿１は、公開鍵ＰＫ＿１がＡＤ内サーバ１００の正しい公開鍵であることを証明するものである。公開鍵証明書Ｃｅｒｔ＿１は、署名データＳｉｇ＿ＣＡ１、公開鍵ＰＫ＿１及びＩＤ＿１を含む。署名データＳｉｇ＿ＣＡ１は、ＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）により、ＡＤ内サーバ１００の公開鍵ＰＫ＿１及びＩＤ＿１に対して署名アルゴリズムＳを施して生成した署名データである。ここでＣＡとは、信頼できる第三者機関であり、グループ形成管理システム１に属する機器の公開鍵の正当性を証明する公開鍵証明書を発行する機関である。なお、署名アルゴリズムＳは、一例として、有限体上のＥｌＧａｍａｌ署名である。ＥｌＧａｍａｌ署名については、公知であるので説明を省略する。

【００２６】
秘密鍵格納部１０２は、外部から内部を見ることが出来ない耐タンパ領域であり、公開鍵ＰＫ＿１に対応する秘密鍵ＳＫ＿１を格納する。

ＣＲＬ格納部１０４は、ＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を格納する。このＣＲＬは、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器のＩＤが登録されたリストであり、ＣＡから発行される。なお、ＣＲＬに登録されるのは、機器のＩＤでなくてもよく、無効化された機器が有する公開鍵証明書のシリアル番号が登録されるとしても良い。ＣＲＬは、放送、インターネット又は

ＤＶＤ等の記録媒体に記録されて各機器へ配布され、各機器は、最新のＣＲＬを入手する。なお、ＣＲＬについては、「American National Standards Institute. American National Standard for financial Services. ANSX9.57:Public Key Cryptography For the Financial Industry: Certificate Management. 1997.」に詳しく開示されている。

【００２７】

コンテンツ格納部１０９は、コンテンツ鍵を用いて暗号化された暗号化コンテンツを格納する。なお、コンテンツの取得方法は、本発明の主題ではないので、説明を省略するが、例として、インターネット、放送などを利用して取得する方法や、ＤＶＤ等の記録媒体から取得する方法が有る。

コンテンツ鍵格納部１１８は、暗号化部１１０から暗号化コンテンツ鍵ａを受け取り、格納する。

（３）公開鍵暗号処理部１０５

公開鍵暗号処理部１０５は、他の機器と通信する際に、認証を行い、ＳＡＣ（Secure Authentication Channel）を確立する。ＳＡＣとは、暗号通信が可能となる安全な通信路を意味する。ＳＡＣを確立する処理によって、認証相手の機器がＣＡに認められた正しい機器であることを確認できる。詳しい確立方法については後述する。また、公開鍵暗号処理部１０５は、認証によって、セッション鍵ＳＫを共有する。

（４）登録情報記憶部１０６

登録情報記憶部１０６は、耐タンパ領域であり、図３（ａ）に示す登録情報を記憶している。登録情報は、ＡＤ内サーバ１００に登録可能な機器の台数及び登録されている機器のＩＤを管理する情報であり、機器ＩＤ、最大、登録台数、残数及びＩＣカードＩＤから構成される。

【００２８】

機器ＩＤは、ＡＤ内サーバ１００に登録された機器のＩＤを記憶する領域である。ＡＤ内サーバ１００に再生装置２００及び車載機器３００が登録されると、図３（ｂ）のように、それぞれのＩＤであるＩＤ＿２及びＩＤ＿３が格納される。

最大は、ＡＤ内サーバ１００に登録可能な機器の最大数を示し、本実施の形態では、２台である。登録台数は、既にＡＤ内サーバ１００に登録されている機器の台数を示す。残数は、ＡＤ内サーバ１００に登録可能な台数を示す。

【００２９】

ＡＤ内サーバ１００にクライアント機器が登録されていない初期の状態では、登録台数は「０」であり、残数は最大と同数である。ＡＤ内サーバ１００に何れかのクライアント機器が登録されると、登録台数に「１」が加算され、残数から「１」が減算される。

ＩＣカードＩＤは、ＡＤ内サーバ１００に付属のＩＣカード４００のＩＤを予め記憶しており、書き換え出来ない。

（５）ＣＳＩ生成部１０７、ＣＳＩ格納部１０８

ＣＳＩ格納部１０８は、外部からＣＳＩを読むことが出来ない耐タンパ領域であり、ＡＤ内サーバ１００に機器が登録されていない場合、未登録であることを示す値として「０」を記憶している。

【００３０】

ＣＳＩ生成部１０７は、制御部１０１の制御の基、ＡＤ内サーバ１００に最初に機器を登録する際に、ＣＳＩを生成する。また、登録した機器が全て脱退すると、ＣＳＩ格納部１０８は、格納している値を「０」に書き換える。

ここでＣＳＩは、ＣＳＩ生成部１０７によって生成される任意のデータであり、本実施の形態では２００ビットとする。なお、ＣＳＩのビット長は、これに限定されず、容易に推測されない、簡単に試すことが不可能な程度の長さであれば良い。

【００３１】
ＣＳＩ生成部１０７は生成したＣＳＩをＣＳＩ格納部１０８に格納する。また、生成したＣＳＩを、接続されているＩＣカード４００に出力する。
なお、ＣＳＩは、定期的又は不定期に更新するとしても良い。
（６）暗号化部１１０、１１９
暗号化部１１９は、再生装置２００の登録の際、制御部１０１の制御の基、公開鍵暗号処理部１０５から受け取るセッション鍵ＳＫを用いて、ＣＳＩに暗号化アルゴリズムＥを施して暗号化ＣＳＩを生成し、生成した暗号化ＣＳＩを入出力部１１５を介して再生装置２００へ送信する。ここで、暗号化アルゴリズムＳは、一例としてＤＥＳである。ＤＥＳについては公知であるので、説明を省略する。
【００３２】
暗号化部１１０は、コンテンツ鍵をコンテンツ鍵格納部１１８に格納する際、ＩＤ格納部１１１からＩＤ＿１を読み出し、ＣＳＩ格納部１０４からＣＳＩを読み出す。読み出したＩＤ＿１及びＣＳＩをこの順で連結して暗号鍵αとし、暗号鍵αを用いてコンテンツ鍵に暗号化アルゴリズムＥを施して暗号化して暗号化コンテンツ鍵αを生成し、生成した暗号化コンテンツ鍵αをコンテンツ鍵格納部１１８へ格納する。
【００３３】
暗号化部１１０は、ＤＶＤ５００に暗号化コンテンツを書き込む際、制御部１０１の制御の基、登録情報記憶部１０６から登録情報の機器ＩＤから登録されている機器のＩＤであるＩＤ＿２及びＩＤ＿３を読み出す。ＩＤ＿２とＣＳＩとをこの順で連結し、暗号鍵βとし、ＩＤ＿３とＣＳＩとをこの順で連結して、暗号鍵γとする。暗号鍵β及び暗号鍵γをそれぞれ用いて暗号化コンテンツ鍵β及び暗号化コンテンツ鍵γを生成し、ＤＶＤ５００に書き込む。
（７）復号部１１７
復号部１１７は、制御部１０１の制御の基、ＩＤ格納部１１１に記憶しているＩＤ＿１を読み出し、ＣＳＩ格納部１０８に格納しているＣＳＩを読み出す。ＩＤ＿１及びＣＳＩをこの順で連結して復号鍵として用い、コンテンツ鍵格納部１１８から読み出した暗号化コンテンツ鍵αに復号アルゴリズムＤを施し、コンテンツ鍵を生成する。生成したコンテンツ鍵は、暗号化部１１０へ出力する。ここで、復号アルゴリズムＤとは、暗号化アルゴリズムＥの逆の処理をするアルゴリズムである。
（８）制御部１０１、入力部１１３、表示部１１４
入力部１１３は、ユーザからの入力を受け付け、受け付けた入力を制御部１０１へ出力する。
【００３４】
制御部１０１は、処理を開始する際、接続されているＩＣカード４００からＩＣカードのＩＤを受信すると、受信したＩＤが登録情報のＩＣカードＩＤと一致するか否かを確認する。一致しない場合は、接続されたＩＣカードが付属のＩＣカードでないことを表示部１１４に表示し、処理を終了する。一致する場合のみ、以降の処理を継続する。
＜再生装置２００の登録＞
再生装置２００から入出力部１１５を介して登録要求を受け取ると、制御部１０１は、公開鍵暗号処理部１０５を制御し、ＣＳＩの初期値「０」を用いて後述の方法でＳＡＣを確立する。ここで、登録の際の認証に使用する「０」は、再生装置２００が、何れのＡＤにも登録されていないことを示す。ＳＡＣを確立する際の機器認証の結果から、相手機器が未登録であるか否かを判断する。認証相手の機器が保持するＣＳＩの値が「０」である場合、認証に成功し、未登録であると判断する。認証相手の機器が保持するＣＳＩの値が、「０」でない場合、制御部１０１は、相手の機器が既に何れかのＡＤに登録されていると判断する。
【００３５】
未登録であると判断した場合、登録情報記憶部１０６から登録情報を読み出し、残数が「０」であるか否かを判断する。残数が「０」でない場合、登録台数が「０」か否かを判

断する。登録台数が「０」の場合、ＣＳＩ生成部１０７を制御してＣＳＩを生成し、ＣＳＩ格納部１０８へ格納する。登録台数が「０」でなかった場合は、ＣＳＩ格納部１０８からＣＳＩを読み出し、生成又は読み出したＣＳＩを暗号化部１１０で暗号化して生成した暗号化ＣＳＩを入出力部１１５を介して、再生装置２００へ出力する。再生装置２００から、ＣＳＩを受け取った事を示す受領通知を受信すると、登録情報の登録台数に「１」を加算し、残数から「１」を減算し、処理を終了する。

【００３６】

機器認証の結果が失敗の場合、相手機器が登録済みである場合及び残数が「０」である場合は、登録できないことを示す登録不可通知を再生装置２００へ送信し、処理を終了する。

また、ＣＳＩ生成部１０７でＣＳＩを生成する際、ＩＣカード４００との間でＳＡＣを確立してセッション鍵ＳＫを共有し、セッション鍵ＳＫを用いて生成したＣＳＩに暗号化アルゴリズムＥを施して暗号化ＣＳＩを生成し、生成した暗号化ＣＳＩをＩＣカード４００へ送信する。

【００３７】

なお、上記登録処理の認証において、認証相手のクライアント機器のＣＳＩが、ＣＳＩ格納部１０８に格納しているＣＳＩと一致するか否かを確認することによって、ＡＤ内サーバ１００が管理するＡＤに登録済みか否かを判断しても良い。クライアント機器の保持するＣＳＩが、ＣＳＩ格納部１０８に格納しているＣＳＩと一致する場合、クライアント機器に対して、既にＡＤ内サーバ１００に登録している旨を通知した後、登録の処理を終了するとしても良い。

【００３８】

また、クライアント機器が保持するＣＳＩが、「０」でなく、ＣＳＩ格納部１０８に格納しているＣＳＩと異なる場合、他のＡＤに登録されていると判断する。クライアント機器が他のＡＤに登録されていると判断する場合、上記登録不可通知を送信後、登録の処理を終了するとしても良い。また、他のＡＤに登録済みであることを通知し、更にＡＤ内サーバ１００への登録を続行するかを尋ね、続行する場合は、上記登録の処理を続行して、ＣＳＩ格納部１０８に格納しているＣＳＩを送信するとしても良い。この場合、クライアント機器は、ＡＤ内サーバ１００からＣＳＩを受信すると、他のＡＤのＣＳＩに、受信したＣＳＩを上書きする。

【００３９】

また、上記登録処理の認証において、クライアント機器を不正な機器でないと判断した場合、クライアント機器が保持するＣＳＩが如何なる値であっても登録処理を行い、ＣＳＩを送信するとしても良い。

＜車載機器３００の登録＞

（ａ）既にＩＤを確認済みのＩＣカード４００が接続された状態で、入力部１１３から、ＣＳＩをコピーする旨の入力を受け付けると、制御部１０１は、残数が「０」か否かを判断し、「０」でなければ、ＩＣカード４００に、ＣＳＩのコピーを１回許可することを示す許可権利を送信する。制御部１０１は、ＩＣカード４００から受領通知を受け取ると、処理を終了する。

【００４０】

残数が「０」の場合は、表示部１１４にコピーできない旨を表示し、処理を終了する。

（ｂ）ＩＣカード４００が接続され、ＩＤを確認し、ＣＳＩをコピーしたことを示すコピー通知を受け取ると、コピー通知に含まれる、ＣＳＩのコピー先のＩＤを抽出し、登録情報に機器ＩＤとして記憶する。また、ＩＣカード４００へ、コピー先のＩＤを受け取ったことを示す受領通知を送信する。

【００４１】

なお、ここでは、既にＣＳＩが生成されているものとして説明したが、ＣＳＩが生成されていない場合は、前述の再生装置２００を登録する際と同様に生成してＩＣカード４００へ送信する。

＜コンテンツ配布＞
入出力部１１５を介して再生装置２００からコンテンツの配送要求を受信すると、制御部１０１は公開鍵暗号処理部１０５を制御して後述の方法でＳＡＣを確立し、セッション鍵ＳＫを共有する。このＳＡＣ確立の際の認証では、ＣＳＩ格納部１０８が格納しているＣＳＩを用いるため、認証に成功した場合、相手機器はＡＤ内サーバ１００が生成したＣＳＩを保持しているので、登録済みであると判断し、認証に失敗した場合、ＡＤ内サーバ１００に登録されていないと判断する。

【００４２】
認証に失敗した場合、コンテンツを配送できないことを示す配送不可通知を再生装置２００へ送信する。
認証に成功した場合、復号部１１７を制御して、コンテンツ鍵格納部１１８に格納している暗号化コンテンツ鍵αを復号する。次に暗号化部１１９を制御して、セッション鍵ＳＫを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵Ｓを生成させ、再生装置２００へ送信する。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し、再生装置２００へ送信する。

＜コンテンツをＤＶＤに記録＞
入力部１１３からコンテンツをＤＶＤ５００に記録する旨の入力を受け付けると、復号部１１７を制御してコンテンツ鍵格納部１１８に格納している暗号化コンテンツ鍵αを復号させてコンテンツ鍵を生成させる。次に、暗号化部１１９を制御して登録情報に登録しているＩＤ＿２及びＩＤ＿３をそれぞれ用いて生成した暗号鍵ｂ及び暗号鍵ｃを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃを生成し、生成した暗号化コンテンツ鍵ｂ及びｃをＤＶＤ５００へ書き込む。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し、ＤＶＤ５００へ書き込む。

【００４３】
なお、ＤＶＤ５００に固有のＩＤを基にして生成した暗号化鍵又はＤＶＤ５００に固有のＩＤ及びＣＳＩを基にして生成した暗号化鍵を用いて、コンテンツ鍵を暗号化するとしても良い。

＜脱退＞
再生装置２００からＩＤ＿２を含む脱退要求を受け取ると、公開鍵暗号処理部１０５を制御して後述の方法でＳＡＣを確立する。この際、ＣＳＩ格納部１０８に格納しているＣＳＩを用いて認証を行う。ＳＡＣ確立の際の認証結果から、要求元の機器が登録済みであるか否かを判断し、未登録の場合脱退できないので、再生装置２００へ未登録であることを示す未登録通知を送信する。

【００４４】
登録済みの場合、再生装置２００へＣＳＩを削除することを示す削除通知を送信する。再生装置２００からＣＳＩの削除が完了したことを示す完了通知を受信すると、登録情報の機器ＩＤからＩＤ＿２を削除し、登録台数から「１」減算し、残数に「１」を加算する。

１．２　再生装置２００の構成
再生装置２００は、図４に示すように、制御部２０１、秘密鍵格納部２０２、公開鍵証明書格納部２０３、ＣＲＬ格納部２０４、公開鍵暗号処理部２０５、ＣＳＩ格納部２０８、コンテンツ格納部２０９、ＩＤ格納部２１１、入力部２１３、入出力部２１５、復号部２１７、暗号化部２１８、コンテンツ鍵格納部２１９、復号部２２０及び再生部２２１から構成される。再生部２２１には、モニタ２５１及びスピーカ２５２が接続されている。

【００４５】
再生装置２００は、ＡＤ内サーバ１００と同様のコンピュータシステムであり、ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、再生装置２００は、その機能を達成する。

（１）入出力部２１５

入出力部２１５は、ＡＤ内サーバ１００とデータの送受信を行う。
（２）秘密鍵格納部２０２、公開鍵証明書格納部２０３、ＣＲＬ格納部２０４、ＣＳＩ格納部２０８、ＩＤ格納部２１１
ＣＲＬ格納部２０４は、最新のＣＲＬを格納している。
【００４６】
ＩＤ格納部２１１は、再生装置２００に固有のＩＤであるＩＤ＿２を記憶している。
ＣＳＩ格納部２０８は、耐タンパ領域であり、未登録であることを示す「０」を格納している。ＡＤ内サーバ１００に登録されると、ＡＤ内サーバ１００より取得したＣＳＩを格納する。
公開鍵証明書格納部２０３は、ＣＡより発行された公開鍵証明書Ｃｅｒｔ＿２を格納する。この公開鍵証明書Ｃｅｒｔ＿２は、再生装置２００の公開鍵ＰＫ＿２及び再生装置２００のＩＤ＿２と、それらに対するＣＡの署名データＳｉｇ＿ＣＡ２とを含む。
【００４７】
秘密鍵格納部２０２は、耐タンパ領域であり、再生装置２００の公開鍵ＰＫ＿２と対応する秘密鍵ＳＫ＿２を格納する。
（３）公開鍵暗号処理部２０５
公開鍵暗号処理部２０５は、ＡＤ内サーバ１００と通信する際に、後述の方法でＳＡＣを確立し、セッション鍵ＳＫを共有する。共有したセッション鍵ＳＫを、復号部２１７へ出力する。
（４）復号部２１７、復号部２２０
復号部２１７は、ＡＤ内サーバ１００からコンテンツを配送される際、公開鍵暗号処理部２０５で共有したセッション鍵ＳＫを用いて、ＡＤ内サーバ１００より配信された暗号化コンテンツ鍵Ｓに、復号アルゴリズムＤを施してコンテンツ鍵を生成する。ここで、復号アルゴリズムＤとは、暗号化アルゴリズムＥと逆の処理を行う。
【００４８】
また、一旦格納したコンテンツを再生する際、ＩＤ格納部２１１からＩＤ＿２を読み出し、ＣＳＩ格納部２０８からＣＳＩを読み出し、ＩＤ＿２及びＣＳＩをこの順で連結して復号鍵ｂを生成する。生成した復号鍵ｂを用いて、コンテンツ鍵格納部２１９から読み出した暗号化コンテンツ鍵ｂに、復号アルゴリズムＤを施してコンテンツ鍵を生成し、生成したコンテンツ鍵を復号部２２０へ出力する。
【００４９】
復号部２２０は、コンテンツ格納部２０９に格納されている暗号化コンテンツを読み出し、復号部２１７から受け取るコンテンツ鍵を用いて、読み出した暗号化コンテンツに復号アルゴリズムＤを施してコンテンツを生成し、生成したコンテンツを再生部２２１へ出力する。
（５）暗号化部２１８
暗号化部２１８は、ＡＤ内サーバ１００から取得したコンテンツを格納する際、ＩＤ格納部２１１からＩＤ＿２を読み出し、ＣＳＩ格納部２０８からＣＳＩを読み出す。ＩＤ＿２及びＣＳＩをこの順で連結して暗号鍵ｂを生成し、生成した暗号鍵ｂを用いて復号部２１７から受け取るコンテンツ鍵に暗号化アルゴリズムＥを施して暗号化コンテンツ鍵ｂを生成し、生成した暗号化コンテンツ鍵ｂをコンテンツ鍵格納部２１９に出力する。
（６）コンテンツ格納部２０９、コンテンツ鍵格納部２１９
コンテンツ格納部２０９は、ＡＤ内サーバ１００から送信される暗号化コンテンツを格納する。
【００５０】
コンテンツ鍵格納部２１９は、暗号化部２１８で暗号化された暗号化コンテンツ鍵ｂを格納する。
（７）制御部２０１、入力部２１３
＜登録＞
入力部２１３が登録処理を開始する旨の入力を受け付けると、制御部２０１は、ＩＤ格

納部２１１からＩＤ＿２を読み出し、ＩＤ＿２を含めた登録要求を、入出力部２１５を介して、ＡＤ内サーバ１００へ送信し、後述の方法でＳＡＣを確立する。

【００５１】

制御部２０１は、ＡＤ内サーバ１００から、登録不可通知を受信すると、モニタ２５１に登録できない旨を表示し、登録の処理を終了する。

制御部２０１は、ＡＤ内サーバ１００から暗号化ＣＳＩを受信すると、復号部２１７を制御して復号させてＣＳＩを生成し、生成したＣＳＩをＣＳＩ格納部２０８に格納する。また、ＣＳＩを受領したことを示す受領通知をＡＤ内サーバ１００へ送信する。

＜コンテンツの配送＞

入力部２１３がコンテンツを取得して再生する旨の入力を受け付けると、制御部２０１は、配送要求をＡＤ内サーバ１００へ送信する。

【００５２】

制御部２０１は、ＡＤ内サーバ１００から配送不可通知を受信すると、モニタ２５１に配送できない旨を表示し、処理を終了する。

受信したコンテンツを再生する場合、制御部２０１は、ＡＤ内サーバ１００から暗号化コンテンツ鍵Ｓを受信すると、復号部２１７を制御して復号させてコンテンツ鍵を生成させる。また、ＡＤ内サーバ１００から暗号化コンテンツを受信すると、復号部２２０を制御し、暗号化コンテンツを復号してコンテンツを生成させ、再生部２２１にコンテンツを再生させる。

＜コンテンツを蓄積してから再生＞

入力部２１３がコンテンツを取得して蓄積する旨の入力を受け付けると、制御部２０１は、上記と同様に処理してコンテンツを取得する。コンテンツを取得すると、制御部２０１は、ＡＤ内サーバ１００から受信した暗号化コンテンツ鍵Ｓを復号部２１７に復号させ、復号したコンテンツ鍵を暗号化部２１８を制御して暗号化させ、暗号化コンテンツ鍵k_bとしてコンテンツ鍵格納部２１９に格納する。また、ＡＤ内サーバ１００から暗号化コンテンツを受信すると、コンテンツ格納部２０９に格納する。

【００５３】

入力部２１３がコンテンツ格納部２０９に格納したコンテンツを再生する旨の入力を受け付けると、制御部２０１は、復号部２１７を制御して暗号化コンテンツ鍵k_bを復号させ、復号部２２０に暗号化コンテンツを復号させてコンテンツを生成し、再生部２２１にコンテンツを再生させる。

＜脱退＞

入力部２１３が脱退処理を開始する旨の入力を受け付けると、制御部１０１は、後述の方法でＳＡＣを確立する。

【００５４】

制御部２０１は、ＡＤ内サーバ１００から未登録通知を受信すると、ＡＤ内サーバ１００に登録されていないことをモニタ２５１に表示して処理を終了する。

制御部２０１は、ＡＤ内サーバ１００から削除通知を受信すると、ＣＳＩ格納部２０８に格納しているＣＳＩを削除し、未登録を示す「０」を格納する。また、削除が完了したことをＡＤ内サーバ１００に通知する削除完了通知を送信する。

（８）再生部２２１

再生部２２１は、復号部２２０から受け取るコンテンツから映像信号を生成し、生成した映像信号をモニタ２５１へ出力する。また、受け取ったコンテンツから音声信号を生成し、生成した音声信号をスピーカ２５２へ出力する。

１．３　車載機器３００の構成

車載機器３００は図５に示すように、制御部３０１、秘密鍵格納部３０２、公開鍵証明書格納部３０３、ＣＲＬ格納部３０４、公開鍵暗号処理部３０５、ＣＳＩ格納部３０８、ＩＤ格納部３１１、ドライブ部３１２、入力部３１３、入出力部３１６、復号部３１７．３１８．３２０、再生部３２１、モニタ３２２及びスピーカ３２３から構成される。

【００５５】

車載機器３００は、ＡＤ内サーバ１００と同様のコンピュータシステムであり、ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、車載機器３００は、その機能を達成する。

（１）ドライブ部３１２、入出力部３１６

ドライブ部３１２は、ＤＶＤ５００から暗号化コンテンツ鍵ｃを読み出し、復号部３１８へ出力する。また、暗号化コンテンツを読み出し、復号部３２０へ出力する。

【００５６】

入出力部３１６は、制御部３０１の制御の基、ＩＣカード４００とデータの送受信を行う。

（２）秘密鍵格納部３０２、公開鍵証明書格納部３０３、ＣＲＬ格納部３０４、ＣＳＩ格納部３０８、ＩＤ格納部３１１

ＣＲＬ格納部３０４は、最新のＣＲＬを格納する。

【００５７】

ＩＤ格納部３１１は、車載機器３００に固有のＩＤであるＩＤ＿３を記憶している。

ＣＳＩ格納部３０８は、耐タンパ領域であり、未登録を示す「０」を格納している。ＩＣカード４００から、ＡＤ内サーバ１００により生成されたＣＳＩを受け取ると、受け取ったＣＳＩを格納する。

公開鍵証明書格納部３０３は、ＣＡより発行された公開鍵証明書Ｃｅｒｔ＿３を格納する。この公開鍵証明書Ｃｅｒｔ＿３は、車載機器３００の公開鍵ＰＫ＿３及びＩＤ＿３と、それらに対するＣＡの署名データＳｉｇ＿ＣＡ３とを含む。

【００５８】

秘密鍵格納部３０２は、耐タンパ領域であり、公開鍵ＰＫ＿３と対応する秘密鍵ＳＫ＿３を格納している。

（３）公開鍵暗号処理部３０５

公開鍵暗号処理部３０５は、制御部３０１の制御の基、ＩＣカード４００と認証を行い、後述の方法でＳＡＣを確立する。また、この際に共有したセッション鍵ＳＫを復号部３１７へ出力する。

（４）復号部３１７．３１８．３２０

復号部３１７は、制御部３０１の制御の基、ＩＣカード４００から暗号化ＣＳＩを受け取ると、公開鍵暗号処理部３０５から受け取るセッション鍵ＳＫを用いて、暗号化ＣＳＩに復号アルゴリズムＤを施してＣＳＩを生成し、生成したＣＳＩをＣＳＩ格納部３０８へ出力する。

【００５９】

復号部３１８は、コンテンツを再生する際、ドライブ部から暗号化コンテンツ鍵ｃを受け取ると、ＩＤ格納部３１１からＩＤ＿３を読み出し、ＣＳＩ格納部３０８からＣＳＩを読み出す。読み出したＩＤ＿３及びＣＳＩをこの順で連結して復号鍵ｃを生成する。復号鍵ｃを用いて暗号化コンテンツ鍵ｃに復号アルゴリズムＤを施してコンテンツ鍵を生成し、生成したコンテンツ鍵を復号部３２０へ出力する。

【００６０】

復号部３２０は、ドライブ部３１２から暗号化コンテンツを受け取り、復号部３１８からコンテンツ鍵を受け取る。受け取ったコンテンツ鍵を用いて暗号化コンテンツに復号アルゴリズムＤを施してコンテンツを生成し、生成したコンテンツを再生部３２１へ出力する。

（５）制御部３０１、入力部３１３

制御部３０１は、ＩＣカード４００が接続されると、ＳＡＣを確立する。この際、ＣＳＩ格納部３０８に格納されている「０」をＣＳＩとして用いる。機器認証に失敗した場合、処理を終了する。また、ＩＣカード４００から登録済通知を受け取った場合、登録済みであることをモニタ３２２に表示して処理を終了する。制御部３０１は、入出力部３１６を介してＩＣカード４００から暗号化ＣＳＩを受け取ると、復号部３１７を制御して復号

させてＣＳＩを生成し、生成したＣＳＩをＣＳＩ格納部３０８に格納する。また、ＣＳＩを受領したことを示す受領通知をＩＣカード４００へ送信する。

【００６１】

なお、車載機器３００から他の機器へのＣＳＩのコピーは行わない。

制御部３０１は、入力部３１３からＤＶＤ５００に記録されているコンテンツを視聴する旨の入力を受け付けると、ドライブ部３１２を制御してＤＶＤ５００から暗号化コンテンツ鍵ｃ及び暗号化コンテンツを読み出す。復号部３１８で暗号化コンテンツ鍵ｃを復号させてコンテンツ鍵を生成させ、復号部３２０で暗号化コンテンツを復号させてコンテンツを生成させる。また、再生部３２１を制御してコンテンツを再生させる。

（６）再生部３２１、モニタ３２２、スピーカ３２３

再生部３２１は、受け取ったコンテンツから映像信号を生成してモニタ３２２へ出力し、音声信号を生成してスピーカ３２３へ出力し、コンテンツを再生する。

１．４　ＩＣカード４００の構成

ＩＣカード４００は図６に示すように、制御部４０１、秘密鍵格納部４０２、公開鍵証明書格納部４０３、ＣＲＬ格納部４０４、公開鍵暗号処理部４０５、ＣＳＩ格納部４０８、ＩＤ格納部４１１、入出力部４１６、復号部４１７、暗号化部４１８及びＩＤ記憶部４２０から構成される。

【００６２】

ＩＣカード４００は、ＡＤ内サーバ１００及び車載機器３００に接続可能である。車載機器３００のような、ＡＤ内サーバ１００と接続できない機器をＡＤ内の機器として登録する際に用いる。

（１）秘密鍵格納部４０２、公開鍵証明書格納部４０３、ＣＲＬ格納部４０４、ＣＳＩ格納部４０８、ＩＤ格納部４１１、ＩＤ記憶部４２０

ＣＲＬ格納部４０４は、最新のＣＲＬを格納する。

【００６３】

ＩＤ格納部４１１は、ＩＣカード４００に固有のＩＤであるＩＤ＿４を記憶している。

ＣＳＩ格納部４０８は、耐タンパ領域であり、ＡＤ内サーバ１００にクライアント機器が登録されていない場合、未登録を示す「０」を格納している。ＡＤ内サーバ１００によりＣＳＩが生成されると、ＡＤ内サーバ１００より取得したＣＳＩと、コピー回数である「０」とを対応付けて記憶する。ここで、コピー回数とは、他のクライアント機器へＣＳＩを通知することを許可された回数である。

【００６４】

公開鍵証明書格納部４０３は、ＣＡより発行された公開鍵証明書Ｃｅｒｔ＿４を格納する。この公開鍵証明書Ｃｅｒｔ＿４は、ＩＣカード４００の公開鍵ＰＫ＿４及びＩＤ＿４と、それらに対するＣＡの署名データＳｉｇ＿ＣＡ４とを含む。

秘密鍵格納部４０２は、耐タンパ領域であり、公開鍵ＰＫ＿４と対応する秘密鍵ＳＫ＿４を格納している。

【００６５】

ＩＤ記憶部４２０は、ＣＳＩのコピー先のＩＤを記憶する領域である。

（２）公開鍵暗号処理部４０５

公開鍵暗号処理部４０５は、制御部４０１の制御の基、ＡＤ内サーバ１００とＳＡＣを確立し、セッション鍵ＳＫを共有し、共有したセッション鍵ＳＫを復号部４１７へ出力する。

【００６６】

また、車載機器３００との間にＳＡＣを確立してセッション鍵ＳＫを共有し、共有したセッション鍵ＳＫを暗号化部４１８へ出力する。

（３）復号部４１７

復号部４１７は、入出力部４１６を介して暗号化ＣＳＩを受け取ると、制御部４０１の制御の基、公開鍵暗号処理部４０５から受け取るセッション鍵ＳＫを用いて暗号化ＣＳＩに復号アルゴリズムＤを施してＣＳＩを生成する。生成したＣＳＩをＣＳＩ格納部４０８

へ格納する。
（４）暗号化部４１８
暗号化部４１８は、制御部４０１の制御の基、ＣＳＩ格納部４０８からＣＳＩを読み出し、公開鍵暗号処理部４０５からセッション鍵ＳＫを受け取り、セッション鍵ＳＫを用いてＣＳＩに暗号化アルゴリズムＥを施して暗号化ＣＳＩを生成し、生成した暗号化ＣＳＩを車載機器３００へ送信する。
（５）制御部４０１、入出力部４１６
ＡＤ内サーバ１００に接続されると、制御部４０１は、ＩＤ格納部４１１からＩＤ＿４を読み出し、読み出したＩＤ＿４をＡＤ内サーバ１００へ送信する。
【００６７】
ＡＤ内サーバ１００からＣＳＩを受け取る際、制御部４０１は、公開鍵暗号処理部４０５を制御してＡＤ内サーバ１００との間にＳＡＣを確立してセッション鍵ＳＫを共有し、暗号化ＣＳＩを受信すると、復号部４１７で復号させてＣＳＩを生成し、ＣＳＩ格納部４０８にＣＳＩを格納する。
車載機器３００を登録する際、制御部４０１は、ＡＤ内サーバ１００から許可権利を受信すると、ＣＳＩと対応付けて格納しているコピー回数に「１」を加算し、ＡＤ内サーバ１００に、受領通知を送信する。
【００６８】
車載機器３００に接続されると、公開鍵暗号処理部４０５を制御してＳＡＣを確立し、セッション鍵ＳＫを共有する。この際、ＣＳＩとして初期値「０」を用いて認証を行い、認証結果から、車載機器３００が未登録であるか否かを判断する。認証が失敗の場合、登録済みであると判断し、登録済通知を送信し、処理を終了する。認証が成功の場合、未登録であると判断し、認証の際に受け取る、車載機器３００のＩＤ＿３をＩＤ記憶部４２０に記憶する。制御部４０１は、ＣＳＩ格納部４０８に格納しているＣＳＩを読み出し、暗号化部４１８で暗号化して暗号化ＣＳＩを生成し、車載機器３００へ送信する。制御部４０１は、車載機器３００から受領通知を受け取ると、コピー回数から「１」減算し、処理を終了する。
【００６９】
制御部４０１は、ＡＤ内サーバ１００に接続されると、ＩＤ格納部４１１からＩＤ＿４を読み出してＡＤ内サーバ１００へ送信する。また、ＩＤ記憶部４２０からＣＳＩのコピー先のＩＤを読み出し、読み出したＩＤを含むコピー通知をＡＤ内サーバ１００へ送信する。ＡＤ内サーバ１００から受領通知を受け取ると、処理を終了する。
２．　グループ形成管理システム１の動作
２．１　ＳＡＣの動作
ＳＡＣを確立する際の動作について、図７．８を用いて説明する。
【００７０】
なお、このＳＡＣの確立方法は、ＡＤ内サーバ１００、再生装置２００、車載機器３００及びＩＣカード４００の何れの機器同士の認証にも利用するため、ここでは認証を行う機器を、機器Ａ及び機器Ｂと称する。また、認証で使用するＣＳＩは、未登録を示す「０」の場合と、ＡＤ内サーバ１００が生成した値の場合とが有るが、ここでは全てＣＳＩとして説明する。
【００７１】
ここで、Ｇｅｎ（）を鍵生成関数とし、Ｙを、システム固有のパラメータとする。また、鍵生成関数Ｇｅｎ（）は、Ｇｅｎ（Ｘ，Ｇｅｎ（Ｙ，Ｚ））＝Ｇｅｎ（Ｙ，Ｇｅｎ（Ｘ，Ｚ））の関係を満たすものとする。なお、鍵生成関数は、任意の公知技術で実現可能なため、その詳細についてここでは言及しない。その一例として、文献（１）池野信一、小山謙二、「現代暗号理論」、電気通信学会にディフィーヘルマン（ＤＨ）型公開鍵配送法が開示されている。
【００７２】
機器Ａは、公開鍵証明書Ｃｅｒｔ＿Ａを読み出し（ステップＳ１１）、機器Ｂへ送信す

る（ステップＳ１２）。

公開鍵証明書Ｃｅｒｔ＿Ａを受け取った機器Ｂは、ＣＡの公開鍵ＰＫ＿ＣＡを用いて、公開鍵証明書Ｃｅｒｔ＿Ａに含まれる署名データＳｉｇ＿ＣＡに対して、署名検証アルゴリズムＶを施して署名検証する（ステップＳ１３）。検証結果が失敗の場合（ステップＳ１４でＮＯ）、処理を終了する。検証結果が成功の場合（ステップＳ１４でＹＥＳ）、ＣＲＬを読み出し（ステップＳ１５）、公開鍵証明書Ｃｅｒｔ＿Ａに含まれて受け取ったＩＤ＿ＡがＣＲＬに登録されているか否かを判断する（ステップＳ１６）。登録されていると判断する場合（ステップＳ１６でＹＥＳ）、処理を終了する。登録されていないと判断する場合（ステップＳ１６でＮＯ）、機器Ｂの公開鍵証明書Ｃｅｒｔ＿Ｂを読み出し（ステップＳ１７）、機器Ａへ送信する（ステップＳ１８）。

【００７３】

機器Ａは、公開鍵証明書Ｃｅｒｔ＿Ｂを受け取ると、公開鍵ＰＫ＿ＣＡを用いて公開鍵証明書Ｃｅｒｔ＿Ｂに含まれる署名データＳｉｇ＿ＣＡに対して、署名検証アルゴリズムＶを施して署名検証する（ステップＳ１９）。検証結果が失敗の場合（ステップＳ２０でＮＯ）、処理を終了する。検証結果が成功の場合（ステップＳ２０ＹＥＳ）、ＣＲＬを読み出し（ステップＳ２１）、公開鍵証明書Ｃｅｒｔ＿Ｂに含まれて受け取ったＩＤ＿ＢがＣＲＬに登録されているか否かを判断する（ステップＳ２２）。登録されていると判断する場合（ステップＳ２２でＹＥＳ）、処理を終了する。登録されていないと判断する場合（ステップＳ２２でＮＯ）、処理を継続する。

【００７４】

機器Ｂは、乱数Ｃｈａ＿Ｂを生成し（ステップＳ２３）、機器Ａへ送信する（ステップＳ２４）。

機器Ａは、乱数Ｃｈａ＿Ｂを受け取ると、Ｃｈａ＿ＢとＣＳＩとをこの順で連結してＣｈａ＿Ｂ｜｜ＣＳＩを生成し（ステップＳ２５）、生成したＣｈａ＿Ｂ｜｜ＣＳＩに、機器Ａの秘密鍵ＳＫ＿Ａを用いて署名生成アルゴリズムＳを施して署名データＳｉｇ＿Ａを生成し（ステップＳ２６）、生成した署名データＳｉｇ＿Ａを機器Ｂへ送信する（ステップＳ２７）。

【００７５】

機器Ｂは、署名データＳｉｇ＿Ａを受け取ると、ステップＳ１２でＣｅｒｔ＿Ａに含んで受け取ったＰＫ＿Ａを用いて受け取った署名データＳｉｇ＿Ａに署名検証アルゴリズムＶを施して署名検証し（ステップＳ２８）、検証結果が失敗の場合は（ステップＳ２９でＮＯ）、処理を終了し、成功の場合（ステップＳ２９でＹＥＳ）は処理を継続する。

機器Ａは、乱数Ｃｈａ＿Ａを生成し（ステップＳ３０）、機器Ｂへ送信する（ステップＳ３１）。

【００７６】

機器Ｂは、受け取ったＣｈａ＿ＡとＣＳＩとをこの順で連結してＣｈａ＿Ａ｜｜ＣＳＩを生成し（ステップＳ３２）、生成したＣｈａ＿Ａ｜｜ＣＳＩに、機器Ｂの秘密鍵ＳＫ＿Ｂを用いて署名生成アルゴリズムＳを施して署名データＳｉｇ＿Ｂを生成し（ステップＳ３３）、生成した署名データＳｉｇ＿Ｂを機器Ａへ送信する（ステップＳ３４）。

機器Ａは、署名データＳｉｇ＿Ｂを受け取ると、ステップＳ１８でＣｅｒｔ＿Ｂに含んで受け取ったＰＫ＿Ｂを用いて署名データＳｉｇ＿Ｂに署名検証アルゴリズムＶを施して署名検証し（ステップＳ３５）、検証結果が失敗の場合（ステップＳ３６でＮＯ）、処理を終了する。成功の場合（ステップＳ３６でＹＥＳ）、乱数「ａ」を生成し（ステップＳ３７）、生成した「ａ」を用いてＫｅｙ＿Ａ＝Ｇｅｎ（ａ，Ｙ）を生成し（ステップＳ３８）、生成したＫｅｙ＿Ａを機器Ｂへ送信する（ステップＳ３９）。

【００７７】

機器Ｂは、Ｋｅｙ＿Ａを受け取ると、乱数「ｂ」を生成し（ステップＳ４０）、生成した乱数「ｂ」を用いてＫｅｙ＿Ｂ＝Ｇｅｎ（ｂ，Ｙ）を生成する（ステップＳ４１）。生成したＫｅｙ＿Ｂを機器Ａへ送信する（ステップＳ４２）。また、生成した乱数「ｂ」と、受け取ったＫｅｙ＿Ａとを用いて、Ｋｅｙ＿ＡＢ＝Ｇｅｎ（ｂ，Ｋｅｙ＿Ａ）＝Ｇｅｎ

（ｂ．Ｇｅｎ（ａ．Ｙ））を生成し（ステップＳ４３）、Ｋｅｙ＿ＡＢと、ＣＳＩとを用いてセッション鍵ＳＫ＝Ｇｅｎ（ＣＳＩ．Ｋｅｙ＿ＡＢ）を生成する（ステップＳ４４）。

【００７８】

機器Ａは、Ｋｅｙ＿Ｂを受け取ると、生成した乱数「ａ」と受け取ったＫｅｙ＿ＢとからＫｅｙ＿ＡＢ＝Ｇｅｎ（ａ．Ｋｅｙ＿Ｂ）＝Ｇｅｎ（ａ．Ｇｅｎ（ｂ．ｙ））を生成し（ステップＳ４５）、生成したＫｅｙ＿ＡＢとＣＳＩとを用いて、セッション鍵ＳＫ＝Ｇｅｎ（ＣＳＩ．Ｋｅｙ＿ＡＢ）を生成する（ステップＳ４６）。

２．２　再生装置２００登録の動作

ＡＤ内サーバ１００に、再生装置２００を登録する際の動作を図９を用いて説明する。

【００７９】

なお、ＡＤ内サーバ１００は、ＩＣカード４００が接続され、ＩＣカード４００が付属のＩＣカードであるかを既に確認している。

再生装置２００は、入力部２１３から登録処理を開始する旨の入力を受け付けると（ステップＳ５１）、ＩＤ格納部２１１からＩＤ＿２を読み出し（ステップＳ５２）、ＩＤ＿２を含めて登録要求をＡＤ内サーバ１００へ送信する（ステップＳ５３）。

【００８０】

ＡＤ内サーバ１００を機器Ａとし、再生装置２００を機器Ｂとして、前述の方法でＳＡＣを確立する（ステップＳ５４）。この際、ＡＤ内サーバ１００は、ＣＳＩとして「０」を使用し、再生装置２００は、ＣＳＩ格納部２０８に格納しているＣＳＩを使用する。

ＡＤ内サーバ１００は、ステップＳ３５の署名検証で、ＣＳＩとして「０」を用いて署名検証するので、検証結果が成功の場合は未登録であると判断し、失敗の場合は、登録済みであると判断する。再生装置２００が未登録であると判断する場合、登録情報を読み出し（ステップＳ５５）、残数が「０」か否かを判断する（ステップＳ５６）。「０」である場合（ステップＳ５６でＹＥＳ）、登録不可通知を再生装置２００へ送信する（ステップＳ５７）。残数が「０」でない場合（ステップＳ５６でＮＯ）、登録台数が「０」であるか否かを判断する（ステップＳ５８）。「０」である場合（ステップＳ５８でＹＥＳ）、ＣＳＩ生成部１０７でＣＳＩを生成する（ステップＳ５９）。登録台数が「０」でない場合（ステップＳ５８でＮＯ）、ＣＳＩ格納部１０８からＣＳＩを読み出す（ステップＳ６０）。生成又は読み出したＣＳＩに、暗号化部１１９でセッション鍵ＳＫを用いて暗号化アルゴリズムＥを施して暗号化して暗号化ＣＳＩを生成し（ステップＳ６１）、暗号化ＣＳＩを再生装置２００へ送信する（ステップＳ６２）。

【００８１】

再生装置２００は、登録不可通知を受信した場合、登録できないことをモニタ２５１に表示し（ステップＳ６３）、処理を終了する。暗号化ＣＳＩを受信した場合、復号部２１７で暗号化ＣＳＩを復号してＣＳＩを生成し（ステップＳ６４）、ＣＳＩ格納部２０８に格納する（ステップＳ６５）。また、ＡＤ内サーバ１００に受領通知を送信する（ステップＳ６６）。

【００８２】

再生装置２００から受領通知を受信すると、登録情報の機器ＩＤに、ＩＤ＿２を書き込み、登録台数に「１」を加算し、残数から「１」を減算する（ステップＳ６７）。

２．３　車載機器３００登録の動作

（１）ＡＤ内サーバ１００からＩＣカード４００にＣＳＩのコピーを許可する際の動作について、図１０を用いて説明する。

【００８３】

ＩＣカード４００がＡＤ内サーバ１００に接続されると、ＩＣカード４００は、ＩＤ格納部４１１からＩＤ＿４を読み出し（ステップＳ７１）、ＡＤ内サーバ１００にＩＤ＿４を送信する（ステップＳ７２）。

ＡＤ内サーバ１００は、ＩＤ＿４を受信すると、登録情報からＩＣカードＩＤを読み出し（ステップＳ７３）、受信したＩＤと読み出したＩＤとが一致するか否かを判断する（

ステップＳ７４）。一致しない場合（ステップＳ７４でＮＯ）、接続されたＩＣカードが付属のＩＣカードでないことを表示部１１４に表示し（ステップＳ７５）、処理を終了する。一致する場合（ステップＳ７４でＹＥＳ）、処理を継続する。このように、接続されたＩＣカードが付属のＩＣカードであるか確認し、確認が済むと入力を受け付けるまで待機する。

【００８４】

入力部１１３が、ＩＣカード４００にＣＳＩを記録する旨の入力を受け付けると（ステップＳ７６）、制御部１０１は、登録情報記憶部１０６から残数を読み出して（ステップＳ７７）、残数が「０」か否かを判断し（ステップＳ７８）、「０」である場合は（ステップＳ７８でＹＥＳ）、登録出来ないことを表示部１１４に表示する（ステップＳ７９）。残数が「０」でない場合（ステップＳ７８でＮＯ）、ＩＣカード４００にＣＳＩのコピーを１回許可する許可権利を送信する（ステップＳ８０）。

【００８５】

ＩＣカード４００は、ＡＤ内サーバ１００から許可権利を受信すると、コピー回数に「１」を加算し（ステップＳ８１）、ＡＤ内サーバ１００に受領通知を送信する（ステップＳ８２）。

ＡＤ内サーバ１００は、受領通知を受信すると、登録情報の登録台数に「１」を加算し、残数から「１」を減算し（ステップＳ８３）、処理を終了する。

（２）ＩＣカード４００から車載機器３００にＣＳＩをコピーする際の動作について、図１１を用いて説明する。

【００８６】

ＩＣカード４００が車載機器３００に接続されると、ステップＳ７１～７５の処理を行い、ＩＣカードＩＤを確信する。また、ＩＣカード４００を機器Ａとして、車載機器３００を機器ＢとしてＳＡＣの確立処理を行い、セッション鍵ＳＫを共有する（ステップＳ９１）。この際、ＩＣカード４００はＣＳＩの初期値である「０」を用いて認証を行い、車載機器３００は、ＣＳＩ格納部３０８に格納している値を用いて認証を行う。

【００８７】

ＩＣカード４００の制御部４０１は、ステップＳ３５の署名検証で、ＣＳＩとして「０」を用いて署名検証するので、検証結果が成功の場合は未登録であると判断し、失敗の場合は、登録済みであると判断する。登録済みと判断する場合（ステップＳ９２でＮＯ）、車載機器３００へ登録不可通知を送信し（ステップＳ９３）、処理を終了する。未登録であると判断する場合（ステップＳ９２でＹＥＳ）、ステップＳ１８で受け取る、車載機器３００のＩＤ＿３をＩＤ記憶部４２０に記憶する（ステップＳ９４）。暗号化部４１８は、公開鍵暗号処理部４０５からセッション鍵ＳＫを受け取ると、ＣＳＩ格納部４０８からＣＳＩを読み出す（ステップＳ９５）。セッション鍵ＳＫを用いてＣＳＩを暗号化して暗号化ＣＳＩを生成し（ステップＳ９６）、生成した暗号化ＣＳＩを入出力部４１６を介して車載機器３００へ送信する（ステップＳ９７）。

【００８８】

車載機器３００の制御部３０１は、ＩＣカード４００から登録不可通知を受け取った場合、登録済みであることをモニタ３２２に表示し（ステップＳ９８）、登録処理を終了する。ＩＣカード４００から暗号化ＣＳＩを受信した場合、復号部３１７は公開鍵暗号処理部３０５からセッション鍵ＳＫを受け取り、セッション鍵ＳＫを用いて暗号化ＣＳＩを復号してＣＳＩを生成し（ステップＳ９９）、生成したＣＳＩをＣＳＩ格納部３０８へ格納する（ステップＳ１００）。また、受領通知をＩＣカード４００へ送信する（ステップＳ１０１）。

【００８９】

ＩＣカード４００は、車載機器３００から受領通知を受信すると、コピー回数から「１」を減算し（ステップＳ１０２）、処理を終了する。

（３）ＣＳＩをコピーしたことをＡＤ内サーバ１００に通知する際の動作

ＩＣカード４００がＡＤ内サーバ１００に接続されると、ＡＤ内サーバ１００は、ＩＣ

カード４００のＩＤを確認して付属のＩＣカードであるか確認し、確認が済むと入力を受け付けるまで待機する。

【００９０】

ＩＣカード４００は、ＩＤ記憶部４２０からコピー先のＩＤであるＩＤ＿３を読み出し、ＩＤ＿３を含むコピー通知をＡＤ内サーバ１００へ送信する。

ＡＤ内サーバ１００は、コピー通知を受信すると、コピー通知に含まれるＩＤ＿３を、登録情報に機器ＩＤとして記憶する。また、ＩＣカード４００へ、受領通知を送信し、処理を終了する。

【００９１】

ＩＣカード４００は、ＡＤ内サーバ１００から受領通知を受信すると、処理を終了する。

２．４　コンテンツ配送の動作１

ＡＤ内サーバ１００から再生装置２００へコンテンツを配信し、再生する際の動作を、図１２を用いて説明する。

【００９２】

再生装置２００は、入力部２１３からコンテンツを取得する旨の入力を受け付けると（ステップＳ１２１）、ＡＤ内サーバ１００へコンテンツの配送要求を送信する（ステップＳ１２２）。

ＡＤ内サーバ１００及び再生装置２００は、ＳＡＣを確立する（ステップＳ１２３）。この際、それぞれＣＳＩ格納部に格納しているＣＳＩを用いて認証を行う。

【００９３】

ＡＤ内サーバ１００は、ステップＳ３５の処理で、再生装置２００が同一ＡＤ内の機器であることを確認する。

認証が失敗の場合（ステップＳ１２４でＮＯ）、ＡＤ内サーバ１００は、再生装置２００へ配送不可通知を送信し（ステップＳ１２５）、処理を終了する。認証が成功の場合（ステップＳ１２４でＹＥＳ）、ＡＤ内サーバ１００は、コンテンツ鍵格納部１１８から暗号化コンテンツ鍵αを読み出し（ステップＳ１２６）、復号部１１７で復号し（ステップＳ１２７）、更に、暗号化部１１０にて、認証の際に共有したセッション鍵ＳＫを用いて暗号化して暗号化コンテンツ鍵Ｓを生成し（ステップＳ１２８）、生成した暗号化コンテンツ鍵Ｓを再生装置２００へ送信する（ステップＳ１２９）。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し（ステップＳ１３０）、再生装置２００へ送信する（ステップＳ１３１）。

【００９４】

再生装置２００は、配送不可通知を受信した場合、モニタ２５１に配送できない旨を表示し（ステップＳ１３２）、処理を終了する。暗号化コンテンツ鍵Ｓを受信した場合、セッション鍵ＳＫを用いて復号部２１７にて復号してコンテンツ鍵を生成し（ステップＳ１３３）、生成したコンテンツ鍵を復号部２２０へ出力する。復号部２２０は、復号部２１７から受け取ったコンテンツ鍵を用いて、ＡＤ内サーバ１００から受け取る暗号化コンテンツに復号アルゴリズムＤを施してコンテンツを生成し（ステップＳ１３４）、再生部２２１へ出力する。再生部２２１は、受け取ったコンテンツから映像信号及び音声信号を生成してモニタ２５１及びスピーカ２５２へ出力し、コンテンツを再生する（ステップＳ１３５）。

２．５　コンテンツ配送の動作２

ＡＤ内サーバ１００から受信したコンテンツを、再生装置２００内に一旦蓄積してから再生する際の動作を、図１３を用いて説明する。

【００９５】

ステップＳ１２１からステップＳ１３０までは同様の処理を行う。

復号部２１７は、暗号化コンテンツ鍵Ｓを復号してコンテンツ鍵を生成し（ステップＳ１４１）、生成したコンテンツ鍵を暗号化部２１８へ出力する。暗号化部２１８は、ＣＳＩ格納部２０８からＣＳＩを読み出し、ＩＤ格納部２１１からＩＤ＿２を読み出す（ステ

ップＳ１４２）。ＩＤ＿２及びＣＳＩをこの順で連結してＩＤ＿２||ＣＳＩを生成し（ステップＳ１４３）暗号化鍵ｂとする。生成した暗号化鍵ｂを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｂを生成し（ステップＳ１４４）、暗号化コンテンツ鍵ｂをコンテンツ鍵格納部２１９へ格納する（ステップＳ１４５）。また、ＡＤ内サーバ１００から暗号化コンテンツを受信すると、コンテンツ格納部２０９へ格納する（ステップＳ１４６）。

【００９６】

入力部２１３から格納したコンテンツを再生する旨の入力を受け付けると（ステップＳ１４７）、復号部２１７は、コンテンツ鍵格納部２１９から暗号化コンテンツ鍵ｂを読み出す（ステップＳ１４８）。また、ＣＳＩ格納部２０８からＣＳＩを読み出し、ＩＤ格納部２１１からＩＤ＿２を読み出し（ステップＳ１４９）、ＩＤ＿２及びＣＳＩを連結してＩＤ＿２||ＣＳＩを生成し（ステップＳ１５０）、復号鍵とする。生成した復号鍵を用いて暗号化コンテンツ鍵ｂに復号アルゴリズムＤを施してコンテンツ鍵を生成し（ステップＳ１５１）、生成したコンテンツ鍵を復号部２２０へ出力する。復号部２２０及び再生部２２１は、ステップＳ１３２～ステップＳ１３３の処理を行い、コンテンツを再生する。

２．６　ＤＶＤに記録する際の動作

ＡＤ内サーバ１００でＤＶＤ５００にコンテンツを書き込む際の動作を、図１４を用いて説明する。

【００９７】

ＡＤ内サーバ１００は、入力部１１３からコンテンツをＤＶＤに記録する旨の入力を受け付けると（ステップＳ１６１）、コンテンツ鍵格納部１１８から暗号化コンテンツ鍵αを読み出し（ステップＳ１６２）、ＩＤ格納部１１１からＩＤ＿１を読み出し、ＣＳＩ格納部１０８からＣＳＩを読み出す（ステップＳ１６３）。復号部１１７は、ＩＤ＿１とＣＳＩとを連結して復号鍵を生成し（ステップＳ１６４）、生成した復号鍵を用いて暗号化コンテンツ鍵αを復号してコンテンツ鍵を生成し（ステップＳ１６５）、生成したコンテンツ鍵を暗号化部１１０へ出力する。暗号化部１１０は、コンテンツ鍵を受け取ると、登録情報記憶部１０６から機器ＩＤを読み出し、ＣＳＩ格納部１０８からＣＳＩを読み出す（ステップＳ１６６）。読み出したＩＤ＿２とＣＳＩとを連結して暗号鍵ｂを生成し、ＩＤ＿３とＣＳＩとを連結して暗号鍵ｃを生成する（ステップＳ１６７）。生成した暗号鍵ｂ及び暗号鍵ｃをそれぞれ用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃを生成する（ステップＳ１６８）。生成した暗号化コンテンツ鍵ｂ及び暗号化コンテンツ鍵ｃをＤＶＤ５００に書き込む（ステップＳ１６９）。また、コンテンツ格納部１０９から暗号化コンテンツを読み出し（ステップＳ１７０）、ＤＶＤ５００に書き込む（ステップＳ１７１）。

２．７　再生装置２００脱退の動作

ＡＤ内サーバ１００から再生装置２００が脱退する際の動作を図１５を用いて説明する。

【００９８】

なお、ＡＤ内サーバ１００は、ＩＣカード４００が接続され、既にＩＣカードＩＤを確認している。

再生装置２００は、入力部２１３から脱退する旨の入力を受け付けると（ステップＳ１８１）、ＩＤ格納部２１１からＩＤ＿２を読み出し（ステップＳ１８２）、ＩＤ＿２を含めて脱退要求をＡＤ内サーバ１００に送信する（ステップＳ１８３）。

【００９９】

ＡＤ内サーバ１００及び再生装置２００は、認証を行い、ＳＡＣを確立する（ステップＳ１８４）。この際、それぞれＣＳＩ格納部に格納しているＣＳＩを用いて認証を行う。

ＡＤ内サーバ１００は、ステップＳ３５の処理で、再生装置２００がＡＤ内の機器として登録しているか否かを判断し、未登録の場合（ステップＳ１８５でＮＯ）、未登録通知を再生装置２００へ送信する（ステップＳ１８６）。登録済みの場合は（ステップＳ１８

５でＹＥＳ）、ＣＳＩ削除通知を送信する（ステップＳ１８７）。

【０１００】

再生装置２００は、未登録通知を受信すると、モニタ３２２に未登録であることを表示し（ステップＳ１８８）、処理を終了する。削除通知を受信すると、ＣＳＩ格納部２０８からＣＳＩを削除する（ステップＳ１８９）。また、削除完了通知をＡＤ内サーバ１００へ送信する（ステップＳ１９０）。

ＡＤ内サーバ１００は、削除完了通知を受信すると、機器ＩＤからＩＤ＿２を削除し、登録台数から「１」を減算し、残数に「１」を加算する（ステップＳ１９１）。

３．　鍵配信方法の変形例

上記のグループ形成管理システム１において、グループ形成後、コンテンツ鍵の配信を行っている。上記に示した鍵配信方法では、コンテンツ鍵の配信時に制限を設けていなかったが、ここでは、コンテンツ鍵の配信時に制限を設けた鍵配信方法について、説明する。

【０１０１】

なお、ここでは、鍵の配信を行うシステムを、鍵配信システムという。

３．１　鍵配信システム１０００の構成

ここでは、鍵配信システム１０００の構成について説明する。

鍵配信システム１０００は、図１６に示すように、コンテンツサーバ１００１、記録媒体１００２、再生装置１００３、再生装置１００４、ゲートウェイ（以下、「ＧＷ」という。）１００７とから構成され、１つのホームネットワークを形成している。このホームネットワークが、上記のグループとなる。ここで、ホームネットワークとは、同一のサブネットが割り当てられているネットワークシステムである。

【０１０２】

ＧＷ１００７は、ネットワーク上で、通信を可能にする機器である。

コンテンツサーバ１００１と再生装置１００３及び再生装置１００４は、ＧＷ１００７を介してホームネットワークを形成しており、さらに、インターネットにより再生装置１００５とネットワーク接続されている。

コンテンツサーバ１００１は、放送局１００６よりコンテンツを受信、又は図示していないが、インターネット上のコンテンツ配信サイトよりコンテンツを取得する。なお、ここでは、便宜上、放送局１００６よりコンテンツを取得することとして話を進める。コンテンツサーバ１００１は、取得したコンテンツを暗号化するためにコンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、取得したコンテンツを暗号化し、暗号化コンテンツを生成し、生成した暗号化コンテンツを、暗号化コンテンツを識別する識別子である情報ＩＤと対応付けて格納する。ここで、コンテンツを暗号化する方法は、共通鍵暗号である。これは、ある情報の暗号化及び復号において、同一の鍵を用いて行うことであり、一例として、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）である。ＡＥＳについては、公知であるので説明を省略する。

【０１０３】

ここで、格納された暗号化コンテンツの複製には、制限を設けない。暗号化コンテンツの複製時には、暗号化コンテンツと情報ＩＤとの組にて複製される。なお、本実施の形態では、再生装置１００４及び記録媒体１００２は、コンテンツサーバ１００１にて生成された暗号化コンテンツを少なくとも１つ以上記憶しているものとする。

また、コンテンツサーバ１００１は、コンテンツ鍵と、コンテンツ鍵を配信できる数とを対応付けて管理することで、暗号化コンテンツの利用を制限する。

【０１０４】

コンテンツサーバ１００１、再生装置１００４及び記録媒体１００２は、鍵配信システム１０００内のみに有効な共通秘密情報を保持しており、コンテンツサーバ１００１は、コンテンツ鍵の配信要求を受け付けた場合には、要求元である再生装置１００４又は記録媒体１００２と、この共通秘密情報を用いて認証を行い、コンテンツ鍵配信の正当性の確認、つまり、配信先の再生装置が正当な装置であるか、又は配信先の記録媒体が正当な記

録媒体であるかを判断する。

【０１０５】

ここで用いる認証方法は、一例として、ゼロ知識証明を利用したチャレンジアンドレスポンス型のハンドシェイクである。この認証方法は、公知であるため説明は省略する。また、認証時には、公開鍵配送法により、共有の秘密鍵（以下、「共有秘密鍵」という。）を生成し、生成した共有秘密鍵を用いて、情報の暗号化及び復号を行う。

認証が成功した場合には、コンテンツサーバ１００１は、コンテンツ鍵の配信要求元へコンテンツ鍵を配信し、配信可能なコンテンツ鍵の数を１減算する。このとき、コンテンツサーバ１００１は、再生装置１００４へコンテンツ鍵の配信を行う場合には、コンテンツ鍵ＩＤとコンテンツ鍵と対応情報ＩＤとからなる第１鍵情報を配信し、再生装置１００４には、第１鍵情報が格納される。ここで、コンテンツ鍵ＩＤとは、コンテンツ鍵を識別する識別子であり、対応情報ＩＤとは、コンテンツ鍵を用いて暗号化された暗号化コンテンツに対応する情報ＩＤである。また、記録媒体１００２へコンテンツ鍵の配信を行う場合には、コンテンツ鍵ＩＤとコンテンツ鍵と対応情報ＩＤと利用期限とからなる第２鍵情報を配信し、記録媒体１００２には、第２鍵情報が格納される。ここで、利用期限とは、コンテンツ鍵の利用可能な期間を示す情報であり、日時を用いて記録されている。なお、コンテンツ鍵ＩＤ、コンテンツ鍵及び対応情報ＩＤは、上記と同様であるため、説明は省略する。

【０１０６】

なお、鍵配信システム１０００外にあるインターネット上の再生装置１００５から、コンテンツサーバ１００１は、コンテンツ鍵の配信要求を受け付け、再生装置１００５と認証を行うが、失敗する。なぜなら、再生装置１００５は、認証部を有している場合には、鍵配信システム１０００内のみに有効な共通秘密情報を保持していないため、コンテンツサーバ１００１との認証は、常に失敗することとなり、認証部を有していない場合も同様に、コンテンツサーバ１００１との認証ができないため、常に失敗することとなる。また、鍵配信システム１０００内のみに有効な共通秘密情報を保持していない記録媒体も同様にコンテンツサーバ１００１との認証は失敗する。

【０１０７】

コンテンツサーバ１００１は、コンテンツ鍵の利用が終了した旨の情報を受け取ると、配信可能なコンテンツ鍵の数を１加算する。

再生装置１００４は、コンテンツサーバ１００１にて暗号化された暗号化コンテンツを記憶しており、記憶している暗号化コンテンツを利用する場合には、コンテンツサーバ１００１へコンテンツ鍵の配信要求を行い、コンテンツサーバ１００１との認証後、認証が成功した場合に、コンテンツサーバ１００１より第１鍵情報を取得し、取得した第１鍵情報に含まれるコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。再生終了後、再生装置１００４は、使用した第１鍵情報を消去し、コンテンツ鍵の利用が終了した旨の情報をコンテンツサーバ１００１へ送信する。

【０１０８】

記録媒体１００２は、ＩＣを内蔵している可搬型の記録媒体であり、例えば、ＩＣを内蔵しているメモリカードである。記録媒体１００２は、コンテンツサーバ１００１にて暗号化された暗号化コンテンツを記憶している。記憶している暗号化コンテンツを利用する場合には、記録媒体１００２は、再生装置１００３へ装着される。再生装置１００３は、暗号化コンテンツの利用時に、記録媒体１００２に利用する暗号化コンテンツに対応する第２鍵情報が存在するか否かの判断を行い、存在する場合には、その第２鍵情報に含まれる利用期限を過ぎているか否かの判断を行い、過ぎていると判断する場合には、再生を行わず、利用期限内であると判断する場合には、その第２鍵情報に含まれるコンテンツ鍵を用いて、利用する暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【０１０９】

記録媒体１００２に利用する暗号化コンテンツに対応する第２鍵情報が存在しないと判断する場合には、コンテンツサーバ１００１へコンテンツ鍵の配信要求を行い、コンテンツサーバ１００１と記録媒体１００２との認証が行われた後、認証が成功した場合に、コンテンツサーバ１００１より第２鍵情報を取得し、取得した第２鍵情報を記録媒体１００２へ格納する。再生装置１００３は、記録媒体１００２へ格納した第２鍵情報に含まれるコンテンツ鍵を用いて、利用する暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【０１１０】

また、コンテンツサーバ１００１は、再生装置１００３と同様の動作にて、記録媒体１００２に記憶されている暗号化コンテンツを利用することができる。さらに、コンテンツサーバ１００１にて記憶している暗号化コンテンツを利用することもできる。この場合、コンテンツ鍵を取得する際の、認証は行わない。

このように、鍵配信システム１０００は、コンテンツサーバ１００１にて、コンテンツ鍵を管理し、鍵配信システム１０００内にコンテンツ鍵の利用を制限、つまり、コンテンツの利用を制限したシステムである。

３．２　コンテンツサーバ１００１の構成

ここでは、コンテンツサーバ１００１の構成について、説明する。

【０１１１】

コンテンツサーバ１００１は、図１７に示すように、コンテンツ記憶部１０１１、管理情報記憶部１０１２、利用鍵記憶部１０１３、受信部１０１４、コンテンツ取得部１０１５、入力部１０１６、再生部１０１７、利用鍵監視部１０１８、利用鍵確認部１０１９、利用鍵事前配信部１０２０、コンテンツ鍵制御部１０２１、認証部１０２２、時間管理部１０２３、入出力部１０２４、通信部１０２５及び時計部１０２６から構成されている。

【０１１２】

コンテンツサーバ１００１は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ネットワークインターフェースなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ１００１は、その機能を達成する。

【０１１３】

（１）　コンテンツ記憶部１０１１

コンテンツ記憶部１０１１は、図１８に一例として示すように、情報ＩＤと暗号化コンテンツを対応付けて記憶するための領域を備えている。

（２）　管理情報記憶部１０１２

管理情報記憶部１０１２は、耐タンパ性を有しており、図１９に示すように、鍵情報記憶部１０３１と、配信鍵情報記憶部１０３２とを備えている。

【０１１４】

鍵情報記憶部１０３１は、図２０に一例として示すように鍵情報テーブルＴ１００１を有している。鍵情報テーブルＴ１００１は、コンテンツ鍵ＩＤ、コンテンツ鍵、対応情報ＩＤ、総数、残数及び制限時間からなる組を１個以上記憶するための領域を備えている。なお、コンテンツ鍵ＩＤ、コンテンツ鍵、対応情報ＩＤ、総数、残数及び制限時間からなる情報をコンテンツ鍵情報と呼ぶ。

【０１１５】

コンテンツ鍵ＩＤは、コンテンツ鍵を識別する識別子である。

コンテンツ鍵は、コンテンツの暗号化に使用した鍵であり、コンテンツ毎に異なる。

対応情報ＩＤは、コンテンツ鍵を用いて暗号化された暗号化コンテンツに対応する情報ＩＤである。これにより、コンテンツ記憶部１０１１に記憶されている暗号化コンテンツと、コンテンツ鍵との対応付けが可能となる。

【０１１６】

総数は、配信可能なコンテンツ鍵と配信されたコンテンツ鍵の和であり、残数は、配信

可能なコンテンツ鍵の数である。

制限時間は、配信されたコンテンツ鍵が利用できる時間が記録されている。記録される時間の単位は、時単位であってもよいし、分単位、秒単位、日単位若しくはこれらの組合せであってもよい。ここでは、時単位で記録されている。

【０１１７】

配信鍵情報記憶部１０３２は、図２１に一例として示すように、配信鍵情報テーブルＴ１００２を有している。

配信鍵情報テーブルＴ１００２は、配信コンテンツ鍵ＩＤと利用期限とからなる組を１個以上記憶するための領域を備えている。なお、配信コンテンツ鍵ＩＤと利用期限とからなる情報をコンテンツ鍵管理情報と呼ぶ。

【０１１８】

配信コンテンツ鍵ＩＤは、記録媒体１００２へ配信したコンテンツ鍵に対応するコンテンツ鍵ＩＤである。

利用期限は、配信されたコンテンツ鍵が利用可能な期限を示し、日時分で記録される。なお、利用期限は、日時分秒であってもよい。

（３） 利用鍵記憶部１０１３

利用鍵記憶部１０１３は、耐タンパ性を有しており、コンテンツサーバ１００１にて、利用中の暗号化コンテンツを復号し、コンテンツを生成するコンテンツ鍵を記憶している。

【０１１９】

（４） 時計部１０２６

時計部１０２６は、日時の計時を行う。

（５） 受信部１０１４

受信部１０１４は、放送局１００６より、放送用に暗号化されたコンテンツを受信し、受信した暗号化されたコンテンツをコンテンツ取得部１０１５へ出力する。

【０１２０】

（６） コンテンツ取得部１０１５

コンテンツ取得部１０１５は、放送用に暗号化されたコンテンツを復号するための復号鍵と、鍵配信システム１０００へ配信可能なコンテンツ鍵の総数及び制限時間を予め記憶している。

コンテンツ取得部１０１５は、受信部１０１４より、放送用に暗号化されたコンテンツを受け取ると、予め記憶している復号鍵を用いて、放送用に暗号化されたコンテンツを復号し、コンテンツを生成する。次に、乱数を用いて、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、生成したコンテンツを暗号化し、暗号化コンテンツを生成する。生成した暗号化コンテンツを識別する情報ＩＤを算出し、算出した情報ＩＤと暗号化コンテンツとをコンテンツ記憶部１０１１へ格納する。

【０１２１】

さらに、コンテンツ取得部１０１５は、生成したコンテンツ鍵を識別するコンテンツ鍵ＩＤを算出し、算出したコンテンツ鍵ＩＤ、情報ＩＤと、生成したコンテンツ鍵と、予め記憶している総数、制限時間とを用いて、コンテンツ鍵情報を生成し、生成したコンテンツ鍵情報を鍵情報テーブルＴ１００１へ書き込む。このとき、残数は、総数と同じ数である。

【０１２２】

（７） 入力部１０１６

入力部１０１６は、コンテンツ利用に係る情報を受け付け、受け付けた情報を再生部１０１７又は利用鍵事前配信部１０２０へ出力する。

入力部１０１６は、利用者より、利用する暗号化コンテンツの格納先が記録媒体１００２であるか否かを示すコンテンツ格納先情報と、利用する暗号化コンテンツに対応する情報ＩＤとを含む再生情報を受け付け、受け付けた再生情報を再生部１０１７へ出力する。ここでは、コンテンツ格納先情報として、「０」、「１」を用いる。「０」の場合には、

利用する暗号化コンテンツの格納先は、記録媒体１００２であることを示す。また、「１」の場合には、それ以外であることを示し、この場合では、利用する暗号化コンテンツの格納先は、コンテンツサーバ１００１であることを示す。

【０１２３】

入力部１０１６は、利用者より、コンテンツの再生を中止する旨を示す再生中止情報を受け付けると、受け付けた再生中止情報を再生部１０１７へ出力する。

また、入力部１０１６は、利用者より、記録媒体１００２へ事前にコンテンツ鍵の配信を要求する旨の事前要求情報を受け付け、受け付けた事前要求情報を利用鍵確認部１０１９へ出力する。ここで、事前要求情報とは、事前に配信を要求するコンテンツ鍵に対応する暗号化コンテンツの情報ＩＤを含む情報である。

【０１２４】

（８）　再生部１０１７

再生部１０１７は、コンテンツ記憶部１０１１に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生、又は記録媒体１００２に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【０１２５】

再生部１０１７は、入力部１０１６より再生情報を受け取り、受け取った再生情報に含まれるコンテンツ格納先情報を用いて、利用する暗号化コンテンツの格納先が記録媒体１００２であるか否かの判断を行う。

利用する暗号化コンテンツの格納先が記録媒体１００２であると判断する場合には、受け取った再生情報を利用鍵確認部１０１９へ出力する。

【０１２６】

利用する暗号化コンテンツの格納先が記録媒体１００２以外、つまり、コンテンツサーバ１００１であると判断する場合には、利用鍵監視部１０１８へ、受け取った再生情報を出力する。

再生部１０１７は、利用鍵監視部１０１８又は利用鍵確認部１０１９より、コンテンツ鍵の格納先が記録媒体１００２であるか否かを示す鍵格納先情報を含む鍵取得完了情報を受け取る。ここでは、鍵格納先情報として、「０」、「１」を用いる。「０」の場合には、コンテンツ鍵の格納先は、記録媒体１００２であることを示す。また、「１」の場合には、それ以外であることを示す。再生部１０１７が受け取った鍵取得完了情報に含まれる鍵格納先情報が「１」である場合には、コンテンツ鍵の格納先は、コンテンツサーバ１００１であることを示す。

【０１２７】

受け取った鍵取得完了情報に含まれる鍵格納先情報を用いて、コンテンツ鍵の格納先が記録媒体１００２であるか否かの判断を行う。

コンテンツ鍵の格納先が記録媒体１００２であると判断する場合には、コンテンツ鍵を記録媒体１００２より入出力部１０２４を介して取得し、さらには、入力部１０１６より受け取った再生情報に含まれる情報ＩＤと対応する暗号化コンテンツを記録媒体１００２より入出力部１０２４を介して取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【０１２８】

コンテンツ鍵の格納先が記録媒体１００２以外、つまり、コンテンツサーバ１００１であると判断する場合には、利用鍵記憶部１０１３に記憶している第１鍵情報に含まれるコンテンツ鍵を取得し、さらには、入力部１０１６より受け取った再生情報に含まれる情報ＩＤと対応する暗号化コンテンツをコンテンツ記憶部１０１１から取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【０１２９】

また、再生部１０１７は、入力部１０１６より再生中止情報を受け取ると、再生中のコ

ンテンツの再生を中止する。

（９） 利用鍵監視部１０１８

利用鍵監視部１０１８は、再生部１０１７にて、コンテンツ記憶部１０１１に記憶している暗号化コンテンツを使用する際に利用する第１鍵情報を利用鍵記憶部１０１３へ格納し、暗号化コンテンツの利用終了時には、格納した第１鍵情報の消去を行う。

【０１３０】

利用鍵監視部１０１８は、再生部１０１７より再生情報を受け取ると、第１要求情報を生成し、生成した第１要求情報をコンテンツ鍵制御部１０２１へ出力する。ここで、第１要求情報とは、コンテンツ鍵を利用鍵記憶部１０１３へ格納する旨の情報であり、再生情報に含まれている情報ＩＤを含んでいる。

利用鍵監視部１０１８は、コンテンツ鍵制御部１０２１より、第１鍵情報を受け取り、受け取った第１鍵情報を利用鍵記憶部１０１３へ格納し、鍵格納先情報が「１」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部１０１７へ出力する。

【０１３１】

さらに、利用鍵監視部１０１８は、再生部１０１７の動作の監視を行い、コンテンツの再生終了若しくは、コンテンツ再生中止により再生部１０１７の動作が終了したこと、つまりコンテンツの利用が終了したことを検知すると、利用鍵記憶部１０１３に記憶している第１鍵情報を消去し、コンテンツ鍵の利用が終了したことを示す鍵利用終了情報を生成し、生成した鍵利用終了情報をコンテンツ鍵制御部１０２１へ出力する。ここで、鍵利用終了情報は、利用した暗号化コンテンツに対応する情報ＩＤを含んでいる。

【０１３２】

（１０） 利用鍵確認部１０１９

利用鍵確認部１０１９は、記録媒体１００２に記録されているコンテンツ鍵の利用期間の確認及びコンテンツ鍵の記録及び消去を行う。

利用鍵確認部１０１９は、再生部１０１７より再生情報を受け取ると、受け取った再生情報に含まれる情報ＩＤと対応する第２鍵情報が存在するか否かの判断を行う。

【０１３３】

第２鍵情報が存在すると判断する場合には、時計部１０２６より、現在の日時を取得し、存在する第２鍵情報に含まれるコンテンツ鍵の利用期限が過ぎているか否かの判断を行う。利用期限内であると判断する場合には、鍵格納先情報が「０」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部１０１７へ出力し、利用期限を過ぎていると判断する場合には、第２鍵情報を消去し、コンテンツ鍵の利用不可を示す利用不可情報を利用者へ通知する。

【０１３４】

第２鍵情報が存在しないと判断する場合には、第２要求情報を生成し、生成した第２要求情報をコンテンツ鍵制御部１０２１へ出力する。また、再生情報を受け取った旨の情報を入出力部１０２４を介して記録媒体１００２へ出力する。ここで、第２要求情報とは、コンテンツ鍵を記録媒体１００２へ出力する旨の情報であり、再生情報に含まれている情報ＩＤを含んでいる。

【０１３５】

利用鍵確認部１０１９は、コンテンツ鍵制御部１０２１より、暗号化された第２鍵情報を受け取り、受け取った暗号化された第２鍵情報を入出力部１０２４を介して記録媒体１００２へ出力する。さらに、利用鍵確認部１０１９は、鍵格納先情報が「０」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部１０１７へ出力する。

（１１） 利用鍵事前配信部１０２０

利用鍵事前配信部１０２０は、記録媒体１００２へ、コンテンツ鍵の事前配信を行う。

【０１３６】

利用鍵事前配信部１０２０は、事前要求情報を受け取ると、受け取った事前要求情報をコンテンツ鍵制御部１０２１へ出力し、さらに、事前要求情報を受け取った旨の情報を入出力部１０２４を介して記録媒体１００２へ出力する。

利用鍵事前配信部１０２０は、コンテンツ鍵制御部１０２１より、暗号化された第２鍵情報を受け取り、受け取った暗号化された第２鍵情報を入出力部１０２４を介して記録媒体１００２へ出力する。

【０１３７】

（１２）　コンテンツ鍵制御部１０２１

コンテンツ鍵制御部１０２１は、配信するコンテンツ鍵の管理を行う。

コンテンツ鍵制御部１０２１は、第１要求情報、第２要求情報、コンテンツ鍵の配信をネットワークを利用して行う旨の第３要求情報、又は事前要求情報を受け付ける。さらに、コンテンツ鍵制御部１０２１は、鍵利用終了情報を利用鍵監視部１０１８又は、通信部１０２５を介して再生装置１００４より受け付ける。

【０１３８】

ここで、第３要求情報は、利用種別と利用する暗号化コンテンツに対応する情報ＩＤとを含んでいる。また、利用種別には、再生装置を示す情報又は記録媒体を示す情報の何れかが記録されている。利用種別として、再生装置を示す情報が記録されている場合には、利用するコンテンツは再生装置に記憶されていることを示し、記録媒体を示す情報が記録されている場合には、利用するコンテンツは記録媒体に記憶されていることを示す。なお、コンテンツ鍵制御部１０２１は、再生装置１００５からの第３要求情報をも受け付ける。

【０１３９】

コンテンツ鍵制御部１０２１は、受け付けた情報が、鍵利用終了情報であるか否かを判断する。

鍵利用終了情報でないと判断する場合には、さらに、第１要求情報であるか否かを判断する。

第１要求情報であると判断する場合には、第１要求情報に含まれる情報ＩＤを用いて、情報ＩＤと一致する対応情報ＩＤを含むコンテンツ鍵情報を鍵情報テーブルＴ１００１より取得する。取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する。「０」であると判断する場合には、コンテンツ鍵の残数が「０」である旨の残数無情報を利用者へ通知する。「０」でないと判断する場合には、取得したコンテンツ鍵情報より第１鍵情報を生成し、生成した第１鍵情報を利用鍵監視部１０１８へ出力する。さらに、コンテンツ鍵制御部１０２１は、取得したコンテンツ鍵情報の残数を１減算して、取得したコンテンツ鍵情報を更新して、鍵情報テーブルＴ１００１へ書き込む。

【０１４０】

第１要求情報でないと判断する場合には、受け付けた情報が第２要求情報、利用種別が再生装置である第３要求情報、利用種別が記録媒体である第３要求情報、又は事前要求情報の何れかであることを示す認証識別情報を認証部１０２２へ出力する。

コンテンツ鍵制御部１０２１は、認証部１０２２から認証が成功した旨の認証成功情報を受け取ると、以下のようにして、コンテンツ鍵の取得、配信及び鍵情報テーブルＴ１００１の更新を行う。

【０１４１】

コンテンツ鍵制御部１０２１は、受け付けた情報が、第２要求情報、第３要求情報、又は事前要求情報の何れかであるかの判断を行う。

第２要求情報であると判断する場合には、第２要求情報に含まれる情報ＩＤを用いて、第１要求情報の場合と同様に、コンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する。「０」であると判断する場合には、コンテンツ鍵の残数が「０」である旨の残数無情報を利用者へ通知する。「０」でないと判断する場合には、さらに、時計部１０２６より現在の日時を取得し、取得した日時とコンテンツ鍵情報に含まれる制限時間とを用いて、利用期限を算出する。算出した利用期限及び取得したコンテンツ鍵情報より第２鍵情報を生成し、生成した第２鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第２鍵情報を利用鍵確認部１０１９へ出力する。さらに、コンテンツ鍵制御部１０２１は、取得したコンテンツ鍵情報の残数を１減算し

て、取得したコンテンツ鍵情報を更新して、鍵情報テーブルＴ１００１へ書き込む。また、コンテンツ鍵制御部１０２１は、算出した利用期限及び取得したコンテンツ鍵情報よりコンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む。

【０１４２】

第３要求情報であると判断する場合には、第３要求情報に含まれる情報ＩＤを用いて、第１要求情報の場合と同様に、コンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する。「０」であると判断する場合には、コンテンツ鍵の残数が「０」である旨の残数無情報を利用者へ通知する。「０」でないと判断する場合には、さらに、第３要求情報に含まれる利用種別が再生装置を示すか又は記録媒体を示すかの判断を行う。

【０１４３】

利用種別が再生装置を示すと判断する場合には、第１鍵情報を生成し、生成した第１鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第１鍵情報を通信部１０２５を介して再生装置１００４へ出力する。さらに、コンテンツ鍵制御部１０２１は、取得したコンテンツ鍵情報の残数を１減算して、取得したコンテンツ鍵情報を更新して、鍵情報テーブルＴ１００１へ書き込む。

【０１４４】

利用種別が記録媒体を示すと判断する場合には、さらに、時計部１０２６より現在の日時を取得し、取得した日時とコンテンツ鍵情報に含まれる制限時間とを用いて、利用期限を算出し、算出した利用期限及び取得したコンテンツ鍵情報より第２鍵情報を生成し、生成した第２鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第２鍵情報を通信部１０２５を介して再生装置１００３に装着された記録媒体１００２へ送信する。さらに、コンテンツ鍵制御部１０２１は、取得したコンテンツ鍵情報の残数を１減算して、取得したコンテンツ鍵情報を更新して、鍵情報テーブルＴ１００１へ書き込む。また、コンテンツ鍵制御部１０２１は、算出した利用期限及び取得したコンテンツ鍵情報よりコンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む。

【０１４５】

事前要求情報であると判断する場合には、事前要求情報に含まれる情報ＩＤを用いて、情報ＩＤと一致する対応情報ＩＤを含むコンテンツ鍵情報を鍵情報テーブルＴ１００１より取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する。「０」であると判断する場合には、コンテンツ鍵の残数が「０」である旨の残数無情報を利用者へ通知する。「０」でないと判断する場合には、さらに、時計部１０２６より現在の日時を取得し、取得した日時とコンテンツ鍵情報に含まれる制限時間とを用いて、利用期限を算出し、算出した利用期限及び取得したコンテンツ鍵情報より第２鍵情報を生成し、生成した第２鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号した第２鍵情報を利用鍵事前配信部１０２０へ出力する。さらに、コンテンツ鍵制御部１０２１は、取得したコンテンツ鍵情報の残数を１減算して、取得した第２鍵情報を更新して、鍵情報テーブルＴ１００１へ書き込む。また、コンテンツ鍵制御部１０２１は、算出した利用期限及び取得したコンテンツ鍵情報よりコンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む。

【０１４６】

コンテンツ鍵制御部１０２１は、受け付けた情報が、鍵利用終了情報であると判断する場合には、受け付けた鍵利用終了情報に含まれる情報ＩＤを用いて、情報ＩＤと一致する対応情報ＩＤを含むコンテンツ鍵情報を鍵情報テーブルＴ１００１より取得する。取得したコンテンツ鍵情報の残数を１加算して、取得したコンテンツ鍵情報を更新し、鍵情報テーブルＴ１００１へ書き込む。

【０１４７】

（１３）　認証部１０２２

認証部１０２２は、予め共通秘密情報を記憶しており、この共通秘密情報を用いて、コンテンツサーバ１００１に装着された記録媒体１００２との認証、再生装置１００４との認証、又は再生装置１００３に装着された記録媒体１００２との認証を行う。

認証部１０２２は、コンテンツ鍵制御部１０２１より認証識別情報を受け取ると、受け取った認証指示情報を用いて、以下のようにして、認証を行う。

【０１４８】

認証識別情報が、第２要求情報又は事前要求情報を示すと判断する場合には、コンテンツサーバ１００１に装着された記録媒体１００２と互いに認証を行う。

利用種別が再生装置である第３要求情報を示すと判断する場合には、再生装置１００４と互いに認証を行い、利用種別が記録媒体である第３要求情報を示すと判断する場合には、再生装置１００３に装着された記録媒体１００２と互いに認証を行う。

【０１４９】

なお、認証部１０２２は、認証開始時に、共有秘密鍵を生成し、生成した共有秘密鍵を用いて、認証に利用する情報を暗号化し、暗号化した情報を再生装置１００４又は記録媒体１００２へ送信し、また、再生装置１００４又は記録媒体１００２から暗号化された情報を受け取り、受け取った暗号化された情報を復号して、復号した情報を認証に利用する。

【０１５０】

認証部１０２２は、認証が成功したか否かの判断を行い、認証が成功した場合には、認証成功情報をコンテンツ鍵制御部１０２１へ出力し、認証が失敗した場合には、認証が失敗した旨の認証失敗情報を利用者へ通知する。

（１４）　時間管理部１０２３

時間管理部１０２３は、時計部１０２６を用いて、配信鍵情報テーブルＴ１００２に記録されている配信コンテンツ鍵ＩＤに対応する利用期限を管理する。

【０１５１】

時間管理部１０２３は、時計部１０２６を用いて、配信鍵情報テーブルＴ１００２に記録されている配信コンテンツ鍵ＩＤに対応する利用期限が過ぎているか否かの判断を行う。利用期限が過ぎていると判断する場合には、そのコンテンツ鍵管理情報を削除し、削除した配信コンテンツ鍵ＩＤと一致するコンテンツ鍵情報を鍵情報テーブルＴ１００１より取得し、取得したコンテンツ鍵情報に含まれる残数に１加算し、コンテンツ鍵情報を更新し、鍵情報テーブルＴ１００１へ書き込む。

【０１５２】

（１５）　入出力部１０２４

入出力部１０２４は、コンテンツサーバ１００１に装着された記録媒体１００２より情報を受け取り、受け取った情報を再生部１０１７、利用鍵確認部１０１９、利用鍵事前配信部１０２０又は認証部１０２２へ出力する。

また、入出力部１０２４は、再生部１０１７、利用鍵確認部１０１９、利用鍵事前配信部１０２０又は認証部１０２２より受け取った情報をコンテンツサーバ１００１に装着された記録媒体１００２へ出力する。

【０１５３】

（１６）　通信部１０２５

通信部１０２５は、コンテンツ鍵制御部１０２１より受け取った情報を再生装置１００４又は、再生装置１００３に装着された記録媒体１００２へ送信し、認証部１０２２より受け取った情報を再生装置１００４、再生装置１００３に装着された記録媒体１００２又は再生装置１００５へ送信する。

【０１５４】

また、通信部１０２５は、再生装置１００４、再生装置１００３に装着された記録媒体１００２又は再生装置１００５より受け取った情報をコンテンツ鍵制御部１０２１又は認証部１０２２へ出力する。

３．３　記録媒体１００２の構成

ここでは、記録媒体１００２の構成について、説明する。

【０１５５】

記録媒体１００２は、図２２に示すように、コンテンツ記憶部１１０１、利用鍵記憶部１１０２、認証部１１０３、及び入出力部１１０４から構成されている。

記録媒体１００２は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、記録媒体１００２は、その機能を達成する。

【０１５６】

（１）　コンテンツ記憶部１１０１

コンテンツ記憶部１１０１は、コンテンツサーバ１００１が備えるコンテンツ記憶部１０１１と同様の領域を備えている。

（２）　利用鍵記憶部１１０２

利用鍵記憶部１１０２は、耐タンパ性を有しており、図２３に一例として示すように、第２鍵情報を１以上記憶するための配信コンテンツ鍵テーブルＴ１１０１を備えている。

【０１５７】

配信コンテンツ鍵テーブルＴ１１０１の各項目については、第２鍵情報を構成するデータと同様であるため、説明は省略する。

（３）　認証部１１０３

認証部１１０３は、予め共通秘密情報を記憶しており、コンテンツサーバ１００１が備える認証部１０２２と認証を行う。

【０１５８】

認証部１１０３は、再生情報又は事前要求情報を受け取った旨の情報を入出力部１１０４を介してコンテンツサーバ１００１から受け取ることにより、又は再生装置１００３が再生情報を受け取った旨の情報を入出力部１１０４を介して再生装置１００３から受け取ることにより、コンテンツサーバ１００１と互いに認証を行う。

認証部１１０３は、認証が成功したか否かの判断を行い、認証が成功した場合には、認証成功情報を入出力部１１０４を介して再生装置１００３へ出力し、認証が失敗した場合には、認証失敗情報を利用者へ通知する。

【０１５９】

また、認証部１１０３は、コンテンツサーバ１００１の認証部１０２２と同様に、認証開始時に、共有秘密鍵を生成する。生成した共有秘密鍵を用いて、認証に利用する情報を暗号化し、暗号化した情報をコンテンツサーバ１００１へ送信し、また、コンテンツサーバ１００１から暗号化された情報を受け取り、受け取った暗号化された情報を復号して、復号した情報を認証に利用する。

【０１６０】

（４）　入出力部１１０４

入出力部１１０４は、記録媒体１００２が装着された装置より情報を受け取る。入出力部１１０４は、受け取った情報が、認証に係る情報であるか、暗号化コンテンツであるか又は暗号化された第２鍵情報であるかの判断を行う。

認証に係る情報であると判断する場合には、認証部１１０３へ出力し、暗号化されたコンテンツであると判断する場合には、コンテンツ記憶部１１０１へ書き込む。暗号化された第２鍵情報であると判断する場合には、認証時に生成された共有秘密鍵を用いて暗号化された第２鍵情報を復号して、第２鍵情報を生成し、生成した第２鍵情報を、利用鍵記憶部１１０２へ書き込む。

【０１６１】

また、入出力部１１０４は、コンテンツ記憶部１１０１、利用鍵記憶部１１０２、又は認証部１１０３より受け取った情報を、記録媒体１００２が装着された装置された装置へ出力する。

３．４　再生装置１００３の構成

ここでは、再生装置１００３の構成について、説明する。

【０１６２】

再生装置１００３は、図２４に示すように、入力部１２０１、再生部１２０２、利用鍵確認部１２０３、入出力部１２０４、通信部１２０５及び時計部１２０６から構成されている。

再生装置１００３は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ネットワークインターフェースなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置１００３は、その機能を達成する。

【０１６３】

（１）　時計部１２０６

時計部１２０６は、日時の計時を行う。

（２）　入力部１２０１

入力部１２０１は、コンテンツ利用に係る情報を受け付け、受け付けた情報を再生部１２０２へ出力する。

【０１６４】

入力部１２０１は、利用者より、再生情報を受け付け、受け付けた再生情報を再生部１２０２へ出力する。ここで、再生情報に含まれるコンテンツ格納先情報は、常に「０」である。

入力部１２０１は、利用者より、コンテンツの再生を中止する旨を示す再生中止情報を受け付けると、受け付けた再生中止情報を再生部１２０２へ出力する。

【０１６５】

（３）　再生部１２０２

再生部１２０２は、記録媒体１００２に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

再生部１２０２は、入力部１２０１より再生情報を受け取ると、受け取った再生情報を利用鍵確認部１２０３へ出力する。

【０１６６】

再生部１２０２は、利用鍵確認部１２０３より、鍵取得完了情報を受け取ると、記録媒体１００２よりコンテンツ鍵を取得し、さらには、入力部１２０１より受け取った再生情報に含まれる情報ＩＤと対応する暗号化コンテンツを記録媒体１００２のコンテンツ記憶部１１０１から取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【０１６７】

また、再生部１２０２は、入力部１２０１より再生中止情報を受け取ると、再生中のコンテンツの再生を中止する。

（４）　利用鍵確認部１２０３

利用鍵確認部１２０３は、記録媒体１００２に記録されているコンテンツ鍵の利用期間の確認及びコンテンツ鍵の記録及び消去を行う。

【０１６８】

利用鍵確認部１２０３は、再生部１２０２より再生情報を受け取ると、受け取った再生情報に含まれる情報ＩＤと対応する第２鍵情報が記録媒体１００２に存在するか否かの判断を行う。

第２鍵情報が存在すると判断する場合には、時計部１２０６より、現在の日時を取得し、存在する第２鍵情報に含まれるコンテンツ鍵の利用期限が過ぎているか否かの判断を行う。利用期限内であると判断する場合には、鍵格納先情報が「０」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部１２０２へ出力する。利用期限を過ぎていると判断する場合には、第２鍵情報を消去し、コンテンツ鍵の利用不可を示す利用不可情報を利用者へ通知する。

【０１６９】
第２鍵情報が存在しないと判断する場合には、記録媒体を示す情報が記録された利用種別と、受け取った再生情報に含まれる情報ＩＤとを含む第３要求情報を生成し、生成した第３要求情報をコンテンツサーバ１００１へ出力する。また、再生情報を受け取った旨の情報を入出力部１０２４を介して記録媒体１００２へ出力する。
利用鍵確認部１２０３は、認証部１１０３より入出力部１２０４を介して、認証成功情報を受け取ると、さらに、通信部１２０５を介してコンテンツサーバ１００１より、暗号化された第２鍵情報を受け取り、受け取った暗号化された第２鍵情報を入出力部１２０４を介して記録媒体１００２へ出力する。さらに、利用鍵確認部１２０３は、鍵格納先情報が「０」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部１２０２へ出力する。
【０１７０】
（５）　入出力部１２０４
入出力部１２０４は、記録媒体１００２より受け取った情報を、再生部１２０２、利用鍵確認部１２０３又は通信部１２０５へ出力する。
また、入出力部１２０４は、再生部１２０２、利用鍵確認部１２０３又は通信部１２０５から受け取った情報を記録媒体１００２へ出力する。
【０１７１】
（６）　通信部１２０５
通信部１２０５は、コンテンツサーバ１００１より受け取った情報を利用鍵確認部１２０３又は入出力部１２０４へ出力する。
また、通信部１２０５は、利用鍵確認部１２０３又は入出力部１２０４より受け取った情報をコンテンツサーバ１００１へ送信する。
３．５　再生装置１００４の構成
ここでは、再生装置１００４の構成について、説明する。
【０１７２】
再生装置１００４は、図２５に示すように、コンテンツ記憶部１３０１、利用鍵記憶部１３０２、入力部１３０３、再生部１３０４、利用鍵監視部１３０５、認証部１３０６及び通信部１３０７から構成されている。
再生装置１００４は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ネットワークインターフェースなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置１００４は、その機能を達成する。
【０１７３】
（１）　コンテンツ記憶部１３０１
コンテンツ記憶部１３０１は、コンテンツサーバ１００１が備えるコンテンツ記憶部１０１１と同様の領域を備えている。
（２）　利用鍵記憶部１３０２
利用鍵記憶部１３０２は、耐タンパ性を有しており、再生装置１００４にて利用中の暗号化コンテンツを復号し、コンテンツを生成するコンテンツ鍵を記憶している。
【０１７４】
（３）　入力部１３０３
入力部１３０３は、コンテンツ利用に係る情報を受け付け、受け付けた情報を再生部１３０４へ出力する。
入力部１３０３は、利用者より、再生情報を受け付け、受け付けた再生情報を再生部１３０４へ出力する。ここで、再生情報に含まれるコンテンツ格納先情報は、常に「１」である。
【０１７５】
入力部１３０３は、利用者より、コンテンツの再生を中止する旨を示す再生中止情報を

受け付けると、受け付けた再生中止情報を再生部１３０４へ出力する。

（４） 再生部１３０４

再生部１３０４は、コンテンツ記憶部１３０１に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【０１７６】

再生部１３０４は、入力部１３０３より再生情報を受け取ると、受け取った再生情報を利用鍵監視部１３０５へ出力する。

再生部１３０４は、利用鍵監視部１３０５より、鍵取得完了情報を受け取ると、利用鍵記憶部１３０２より第１鍵情報に含まれるコンテンツ鍵を取得し、さらには、入力部１３０３より受け取った再生情報に含まれる情報ＩＤと対応する暗号化コンテンツをコンテンツ記憶部１３０１から取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【０１７７】

また、再生部１３０４は、入力部１３０３より再生中止情報を受け取ると、再生中のコンテンツの再生を中止する。

（５） 利用鍵監視部１３０５

利用鍵監視部１３０５は、再生部１３０４にてコンテンツ記憶部１３０１に記憶している暗号化コンテンツを使用する際に利用するコンテンツ鍵を利用鍵記憶部１３０２へ格納し、暗号化コンテンツの利用終了時には、格納したコンテンツ鍵の消去を行う。

【０１７８】

利用鍵監視部１３０５は、再生部１３０４より再生情報を受け取ると、再生装置を示す情報が記録された利用種別と、受け取った再生情報に含まれる情報ＩＤとを含む第３要求情報を生成し、生成した第３要求情報をコンテンツサーバ１００１へ出力し、さらに、再生情報を受け取った旨の情報を認証部１３０６へ出力する。

利用鍵監視部１３０５は、認証部１３０６より認証成功情報を受け取ると、さらに、コンテンツサーバ１００１より通信部１３０７を介して、暗号化された第１鍵情報を受け取る。利用鍵監視部１３０５は、認証時に生成された共有秘密鍵を用いて、受け取った暗号化された第１鍵情報を復号して、第１鍵情報を生成し、生成した第１鍵情報を利用鍵記憶部１３０２へ格納する。さらに、利用鍵監視部１３０５は、鍵格納先情報が「１」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部１３０４へ出力する。この場合、鍵格納先情報が「１」である場合には、コンテンツ鍵の格納先は、再生装置１００４の利用鍵記憶部１３０２であることを示す。

【０１７９】

さらに、利用鍵監視部１３０５は、再生部１３０４の動作の監視を行い、コンテンツの再生終了若しくは、コンテンツ再生中止により再生部１３０４の動作が終了したこと、つまりコンテンツの利用が終了したことを検知すると、利用鍵記憶部１３０２に記憶している第１鍵情報を消去し、鍵利用終了情報を生成し、生成した鍵利用終了情報をコンテンツサーバ１００１へ出力する。

【０１８０】

（６） 認証部１３０６

認証部１３０６は、予め共通秘密情報を記憶しており、コンテンツサーバ１００１が備える認証部１０２２と認証を行う。

認証部１３０６は、利用鍵監視部１３０５より再生情報を受け取った旨の情報を受け取ることにより、コンテンツサーバ１００１と互いに認証を行う。

【０１８１】

認証部１３０６は、認証が成功したか否かの判断を行い、認証が成功した場合には、認証成功情報を利用鍵監視部１３０５へ出力し、認証が失敗した場合には、認証が失敗した旨の認証失敗情報を利用者へ通知する。

また、認証部１３０６は、コンテンツサーバ１００１の認証部１０２２と同様に、認証開始時に、共有秘密鍵を生成する。生成した共有秘密鍵を用いて、認証に利用する情報を

暗号化し、暗号化した情報をコンテンツサーバ１００１へ送信し、また、コンテンツサーバ１００１から暗号化された情報を受け取り、受け取った暗号化された情報を復号して、復号した情報を認証に利用する。

【０１８２】

（７）　通信部１３０７

通信部１３０７は、コンテンツサーバ１００１より受信した情報を利用鍵監視部１３０５又は認証部１３０６へ出力する。

また、通信部１３０７は、利用鍵監視部１３０５又は認証部１３０６より受け取った情報をコンテンツサーバ１００１へ出力する。

３．６　鍵配信システム１０００の動作

ここでは、鍵配信システム１０００の動作について、説明する。

【０１８３】

（１）　コンテンツ鍵管理処理

ここでは、コンテンツサーバ１００１のコンテンツ鍵制御部１０２１と認証部１０２２とで行われるコンテンツ鍵管理処理について、図２６及び図２７の流れ図を用いて説明する。

コンテンツ鍵制御部１０２１は、情報を受け付け（ステップＳ１０００）、受け付けた情報が、鍵利用終了情報であるか否かの判断を行う（ステップＳ１００５）。

【０１８４】

ステップＳ１００５にて鍵利用終了情報であると判断する場合には、受け付けた鍵利用終了情報に含まれる情報ＩＤを用いて、情報ＩＤに対応するコンテンツ鍵情報の残数を１加算して、鍵情報テーブルＴ１００１の更新を行う（ステップＳ１０１０）。

ステップＳ１００５にて鍵利用終了情報でないと判断する場合には、受け付けた情報が、第１要求情報であるか否かを判断する（ステップＳ１０１５）。

【０１８５】

ステップＳ１０１５にて第１要求情報であると判断する場合には、第１要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１０２０）。

ステップＳ１０２０にて残数が「０」でないと判断する場合には、取得したコンテンツ鍵情報より第１鍵情報を生成し、生成した第１鍵情報を利用鍵監視部１０１８へ出力する（ステップＳ１０２５）。さらに、取得したコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１０３０）。

【０１８６】

ステップＳ１０２０にて、残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１１３５）。

ステップＳ１０１５にて第１要求情報でないと判断する場合には、コンテンツ鍵制御部１０２１は、認証識別情報を認証部１０２２へ出力し、認証部１０２２にて、コンテンツ鍵の配信要求元と認証処理を行う（ステップＳ１０３５）。ステップＳ１０３５にて行われた認証処理が成功したか否かを判断する（ステップＳ１０４０）。ステップＳ１０４０にて認証が失敗と判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１０４５）。

【０１８７】

ステップＳ１０４０にて認証が成功と判断する場合には、受け付けた情報が、第２要求情報であるか否かを判断する（ステップＳ１０５０）。

ステップＳ１０５０にて第２要求情報であると判断する場合には、第２要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１０５５）。

【０１８８】

ステップＳ１０５５にて残数が「０」でないと判断する場合には、取得したコンテンツ鍵情報より第２鍵情報を生成し、生成した第２鍵情報を暗号化して、暗号化した第２鍵情

報を利用鍵確認部１０１９へ出力する（ステップＳ１０６０）。さらに、取得したコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１０６５）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む（ステップＳ１０７０）。

【０１８９】

ステップＳ１０５５にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１１３５）。

ステップＳ１０５０にて第２要求情報でないと判断する場合には、受け付けた情報が第３要求情報であるか否かを判断する（ステップＳ１０７５）。

ステップＳ１０７５にて第３要求情報であると判断する場合には、第３要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１０８０）。

【０１９０】

ステップＳ１０８０にて残数が「０」でないと判断する場合には、受け付けた第３要求情報に含まれる利用種別が再生装置を示す情報であるか否かを判断する（ステップＳ１０８５）。

ステップＳ１０８５にて再生装置を示す情報であると判断する場合には、取得したコンテンツ鍵情報より第１鍵情報を生成し、生成した第１鍵情報を暗号化して、暗号化した第１鍵情報を再生装置１００４へ送信する（ステップＳ１０９０）。さらに、取得したコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１０６５）。

【０１９１】

ステップＳ１０８５にて再生装置を示す情報でないと判断する場合には、取得したコンテンツ鍵情報より第２鍵情報を生成し、生成した第２鍵情報を暗号化して、暗号化した第２鍵情報を記録媒体１００２へ送信する（ステップＳ１１００）。さらに、取得したコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１１０５）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む（ステップＳ１１１０）。

【０１９２】

ステップＳ１０８０にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１１３５）。

ステップＳ１０７５にて第３要求情報でないと判断する、つまり、受け付けた情報が事前要求情報であると判断する場合には、受け付けた事前要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１１１５）。

【０１９３】

ステップＳ１１１５にて残数が「０」でないと判断する場合には、取得したコンテンツ鍵情報より第２鍵情報を生成し、生成した第２鍵情報を暗号化して、暗号化した第２鍵情報を利用鍵事前配信部１０２０へ出力する（ステップＳ１１２０）。さらに、取得したコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１１２５）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む（ステップＳ１１３０）。

【０１９４】

ステップＳ１１１５にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１１３５）。

（２）　認証処理の動作

ここでは、コンテンツ鍵管理処理にて行われる認証処理について、図２８の流れ図を用いて説明する。

【０１９５】

認証部１０２２は、コンテンツ鍵制御部１０２１より、認証識別情報を受け取ると、受

け取った認証識別情報が、第２要求情報又は事前要求情報を示すか否かを判断する（ステップＳ１１５０）。

第２要求情報又は事前要求情報を示すと判断する場合には、コンテンツサーバ１００１に装着された記録媒体１００２と、互いに認証を行う（ステップＳ１１５５）。

【０１９６】

ステップＳ１１５０にて、受け取った認証識別情報が、第２要求情報を示す情報でなく、且つ事前要求情報示す情報でないと判断する場合には、利用種別が再生装置である第３要求情報であるか否かを判断する（ステップＳ１１６０）。

利用種別が再生装置である第３要求情報を示すと判断する場合には、再生装置１００４と、互いに認証を行い（ステップＳ１１６５）、利用種別が再生装置である第３要求情報でないと判断する場合、つまり、利用種別が記録媒体である第３要求情報を示すと判断する場合には、再生装置１００３に装着された記録媒体１００２と、互いに認証を行う（ステップＳ１１７０）。

【０１９７】

（３）　時間管理処理

ここでは、コンテンツサーバ１００１の時間管理部１０２３にて行われる時間管理処理について、図２９の流れ図を用いて説明する。

時間管理部１０２３は、配信鍵情報テーブルＴ１００２よりコンテンツ鍵管理情報の取得と、時計部１０２６より現在の日時の取得を行い（ステップＳ１２００）、取得した日時を用いて、コンテンツ鍵管理情報に含まれる利用期限を過ぎているか否かを判断する（ステップＳ１２０５）。

【０１９８】

ステップＳ１２０５にて利用期限が過ぎていると判断する場合には、取得したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２より削除し（ステップＳ１２１０）、取得したコンテンツ鍵管理情報の配信コンテンツ鍵ＩＤと対応するコンテンツ鍵情報の残数を１加算して、鍵情報テーブルＴ１００１の更新を行う（ステップＳ１２１５）。

なお、この処理を配信鍵情報テーブルＴ１００２に記憶されているコンテンツ鍵管理情報の数分繰り返す。

【０１９９】

（４）　再生装置１００４における再生時の動作

ここでは、再生装置１００４に記憶されている暗号化コンテンツを利用する場合の動作について、図３０に示す流れ図を用いて説明する。

再生装置１００４は、再生情報を受け付けると（ステップＳ１２５０）、再生装置を示す利用種別を含む第３要求情報を生成し、生成した第３要求情報をコンテンツサーバ１００１へ送信する（ステップＳ１２５５）。

【０２００】

コンテンツサーバ１００１は、第３要求情報を受信すると（ステップＳ１２６０）、再生装置１００４と互いに認証を行う（ステップＳ１２６５、ステップＳ１２７０）。

コンテンツサーバ１００１は、再生装置１００４との認証が成功したか否かの判断を行う（ステップＳ１２７５）。

コンテンツサーバ１００１は、ステップＳ１２７５にて認証が成功したと判断する場合には、第３要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１２８５）。ステップＳ１２７５にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１３４０）。

【０２０１】

コンテンツサーバ１００１は、ステップＳ１２８５にて残数が「０」でないと判断する場合には、第１鍵情報を生成し、生成した第１鍵情報を暗号化して、再生装置１００４へ送信する（ステップＳ１２９０）。ステップＳ１２８５にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１３４５）。

コンテンツサーバ１００１は、第３要求情報に含まれる情報ＩＤに対応するコンテンツ

鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１２９５）。

【０２０２】

再生装置１００４は、認証が成功したか否かを判断する（ステップＳ１２８０）。

再生装置１００４は、ステップＳ１２８０にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１３３５）。認証が成功したと判断する場合には、コンテンツサーバ１００１より暗号化された第１鍵情報を受信し、暗号化された第１鍵情報を復号して、第１鍵情報を生成する（ステップＳ１３００）。

【０２０３】

再生装置１００４は、生成した第１鍵情報を利用鍵記憶部１３０２へ格納し（ステップＳ１３０５）、格納した第１鍵情報と、コンテンツ記憶部１３０１に記憶されている暗号化コンテンツとを用いて、コンテンツを再生する（ステップＳ１３１０）。また、コンテンツ利用終了を検知すると（ステップＳ１３１５）、利用鍵記憶部１３０２へ格納した第１鍵情報を消去し（ステップＳ１３２０）、鍵利用終了情報生成し、生成した鍵終了情報をコンテンツサーバ１００１へ送信する（ステップＳ１３２５）。

【０２０４】

コンテンツサーバ１００１は、再生装置１００４より鍵利用終了情報を受信すると、受信した鍵利用終了情報に含まれる情報ＩＤを用いて、情報ＩＤに対応するコンテンツ鍵情報の残数を１加算して、鍵情報テーブルＴ１００１の更新を行う（ステップＳ１３３０）。

（５）　再生装置１００３における再生時の動作

ここでは、記録媒体１００２に記憶されている暗号化コンテンツを再生装置１００３にて利用する場合の動作について、図３１に示す流れ図を用いて説明する。

【０２０５】

再生装置１００３は、再生情報を受け付けると（ステップＳ１４００）、受け付けた再生情報に含まれる情報ＩＤに対応する第２鍵情報が記録媒体１００２に存在するか否かの撤断を行う（ステップＳ１４０５）。

ステップＳ１４０５にて第２鍵情報が存在すると判断する場合には、鍵確認処理を行う（ステップＳ１４１０）。

【０２０６】

ステップＳ１４０５にて第２鍵情報が存在しないと判断する場合には、記録媒体を示す利用種別を含む第３要求情報を生成し、生成した第３要求情報をコンテンツサーバ１００１へ送信する（ステップＳ１４１５）。

コンテンツサーバ１００１は、第３要求情報を受信すると（ステップＳ１４２０）、記録媒体１００２と互いに認証を行う（ステップＳ１４２５、ステップＳ１４３０）。

【０２０７】

コンテンツサーバ１００１は、記録媒体１００２との認証が成功したか否かの判断を行う（ステップＳ１４３５）。

コンテンツサーバ１００１は、ステップＳ１４３５にて認証が成功したと判断する場合には、第３要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１４４５）。ステップＳ１４３５にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１４８５）。

【０２０８】

コンテンツサーバ１００１は、ステップＳ１４４５にて残数が「０」でないと判断する場合には、第２鍵情報を生成し、生成した第２鍵情報を暗号化して、再生装置１００３へ送信する（ステップＳ１４５０）。ステップＳ１４４５にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１４９０）。

コンテンツサーバ１００１は、第３要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１４５５）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報

テーブルＴ１００２に書き込む（ステップＳ１４６０）。

【０２０９】

記録媒体１００２は、認証が成功したか否かを判断する（ステップＳ１４４０）。

記録媒体１００２は、ステップＳ１４３０にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１４８０）。認証が成功したと判断する場合には、再生装置１００３へ認証成功情報を出力し、再生装置１００３は、コンテンツサーバ１００１より暗号化された第２鍵情報を受信し、受信した暗号化された第２鍵情報を記録媒体１００２へ出力する（ステップＳ１４６５）。

【０２１０】

記録媒体１００２は、再生装置１００３より暗号化された第２鍵情報を受け取り、受け取った暗号化された第２鍵情報を復号して、第２鍵情報を生成し、生成した第２鍵情報を利用鍵記憶部１１０２へ格納する（ステップＳ１４７０）。

再生装置１００３は、記録媒体１００２に格納されている第２鍵情報と暗号化コンテンツとを用いて、コンテンツを再生する（ステップＳ１４７５）。

【０２１１】

（６）　コンテンツサーバ１００１にて記録媒体１００２の利用時の動作

ここでは、記録媒体１００２に記憶されている暗号化コンテンツをコンテンツサーバ１００１にて利用する場合の動作について、図３２に示す流れ図を用いて説明する。

コンテンツサーバ１００１は、格納先情報が「０」である再生情報を受け付けると（ステップＳ１５００）、受け付けた再生情報に含まれる情報ＩＤに対応する第２鍵情報が記録媒体１００２に存在するか否かの判断を行う（ステップＳ１５０５）。

【０２１２】

ステップＳ１５０５にて第２鍵情報が存在すると判断する場合には、鍵確認処理を行う（ステップＳ１５１０）。

ステップＳ１５０５にて第２鍵情報が存在しないと判断する場合には、記録媒体１００２と互いに認証を行う（ステップＳ１５１５、ステップＳ１５２０）。

コンテンツサーバ１００１は、記録媒体１００２との認証が成功したか否かの判断を行う（ステップＳ１５２５）。

【０２１３】

コンテンツサーバ１００１は、ステップＳ１４３５にて認証が成功したと判断する場合には、受け付けた再生情報を用いて生成した第２要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１５３５）。ステップＳ１５２５にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１５６５）。

【０２１４】

コンテンツサーバ１００１は、ステップＳ１５３５にて残数が「０」でないと判断する場合には、第２鍵情報を生成し、生成した第２鍵情報を暗号化して、暗号化した第２鍵情報を記録媒体１００２へ出力する（ステップＳ１５４０）。ステップＳ１５３５にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１５７０）。

【０２１５】

コンテンツサーバ１００１は、第２要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１５４５）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む（ステップＳ１５５０）。さらに、コンテンツサーバ１００１は、記録媒体１００２へ出力した第２鍵情報と、暗号化コンテンツとを記録媒体１００２より読み出し、コンテンツを再生する（ステップＳ１５５５）。

【０２１６】

記録媒体１００２は、認証が成功したか否かを判断する（ステップＳ１５２０）。

記録媒体１００２は、ステップＳ１５２０にて認証が失敗したと判断する場合には、認

証失敗情報を利用者へ通知する（ステップＳ１５７５）。認証が成功したと判断する場合には、コンテンツサーバ１００１より暗号化された第２鍵情報を受け取り、受け取った暗号化された第２鍵情報を復号して、第２鍵情報を生成し、生成した第２鍵情報を利用鍵記憶部１１０２へ格納する（ステップＳ１５６０）。

【０２１７】

（７）　コンテンツサーバ１００１の再生動作

ここでは、コンテンツサーバ１００１に記憶されている暗号化コンテンツを再生する場合の動作について、図３３に示す流れ図を用いて説明する。

コンテンツサーバ１００１は、格納先情報が「１」である再生情報を受け付けると（ステップＳ１６００）、受け付けた再生情報を用いて生成した第１要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１６０５）。

【０２１８】

コンテンツサーバ１００１は、ステップＳ１６０５にて残数が「０」でないと判断する場合には、第１鍵情報を生成し、生成した第１鍵情報を利用鍵記憶部１０１３へ格納する（ステップＳ１６１０）。ステップＳ１６０５にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１６４０）。

コンテンツサーバ１００１は、第１要求情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１６１５）。さらに、コンテンツサーバ１００１は、第１鍵情報と、暗号化コンテンツとを用いて、コンテンツを利用する（ステップＳ１６２０）。また、コンテンツ利用終了を検知すると（ステップＳ１６２５）、利用鍵記憶部１０１３へ格納した第１鍵情報を消去し（ステップＳ１６３０）、利用した暗号化コンテンツの情報ＩＤに対応するコンテンツ鍵情報の残数を１加算して、鍵情報テーブルＴ１００１の更新を行う（ステップＳ１６３５）。

【０２１９】

（８）　鍵確認処理の動作

ここでは、図３１にて示した鍵確認処理の動作について、図３４に示す流れ図を用いて説明する。鍵確認処理は、再生装置１００３の再生部１２０２及び利用鍵確認部１２０３にて行われる処理である。

利用鍵確認部１２０３は、存在する第２鍵情報に含まれるコンテンツ鍵が、利用期限を過ぎているか否かの判断を行う（ステップＳ１６６０）。利用期限内であると判断する場合には、再生部１２０２は、当該コンテンツ鍵を取得し、取得したコンテンツ鍵を用いて暗号化コンテンツを復号し、コンテンツを生成して、生成したコンテンツを再生する（ステップＳ１６７０）。

【０２２０】

利用期限でないと判断する場合には、利用鍵確認部１２０３は、当該コンテンツ鍵を含む第２鍵情報を削除し（ステップＳ１６７５）、利用不可情報を利用者へ通知する（ステップＳ１６８０）。

なお、図３２にて示した鍵配信処理の動作についても同様であるため、説明は省略する。この場合の鍵配信処理は、コンテンツサーバ１００１の再生部１０１７及び利用鍵確認部１０１９にて行われる。

【０２２１】

（９）　コンテンツ鍵の事前配信時の動作

ここでは、記録媒体１００２へコンテンツ鍵を事前に配信する場合の動作について、図３５に示す流れ図を用いて説明する。

コンテンツサーバ１００１は、事前要求情報を受け付けると、記録媒体１００２へ事前要求情報を受け取った旨の情報を出力する（ステップＳ１７００）。

【０２２２】

記録媒体１００２は、コンテンツサーバ１００１より事前要求情報を受け取った旨の情報を受け取り（ステップＳ１７０５）、コンテンツサーバ１００１と互いに認証を行う（

ステップＳ１７１０、ステップＳ１７１５）

コンテンツサーバ１００１は、記録媒体１００２との認証が成功したか否かの判断を行う（ステップＳ１７２０）。

【０２２３】

コンテンツサーバ１００１は、ステップＳ１７２０にて認証が成功したと判断する場合には、受け付けた事前配信情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数が「０」であるか否かを判断する（ステップＳ１７３０）。ステップＳ１７２０にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１７５５）。

【０２２４】

コンテンツサーバ１００１は、ステップＳ１７３０にて残数が「０」でないと判断する場合には、第２鍵情報を生成し、生成した第２鍵情報を暗号化して、暗号化した第２鍵情報を記録媒体１００２へ出力する（ステップＳ１７３５）。ステップＳ１７３０にて残数が「０」であると判断する場合には、残数無情報を利用者へ通知する（ステップＳ１７６０）。

【０２２５】

コンテンツサーバ１００１は、受け付けた事前配信情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数を１減算して、鍵情報テーブルＴ１００１を更新する（ステップＳ１７４０）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルＴ１００２に書き込む（ステップＳ１７４５）。

記録媒体１００２は、認証が成功したか否かを判断する（ステップＳ１７２５）。

【０２２６】

記録媒体１００２は、ステップＳ１７２５にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップＳ１７６５）。認証が成功したと判断する場合には、コンテンツサーバ１００１より暗号化された第２鍵情報を受け取り、受け取った暗号化された第２鍵情報を復号して、第２鍵情報を生成し、生成した第２鍵情報を利用鍵記憶部１１０２へ格納する（ステップＳ１７５０）。

３．７　鍵配信方法の変形例のまとめ

以上説明したように、鍵配信システム１０００におけるコンテンツサーバ１００１は、認証により鍵配信の正当性が確認され、配信要求のあったコンテンツ鍵の残数が０でない場合に、コンテンツ鍵の配信を行う。また、記録媒体１００２へコンテンツ鍵を配信する場合には、コンテンツ鍵を利用することができる利用期間を付加することにより、記録媒体１００２配信されたコンテンツ鍵の利用を制限する。これにより、常にネットワーク接続されない記録媒体１００２に対してコンテンツの利用を制限することができる。

３．８　変形例

上記に説明した鍵配信方法の変形例は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【０２２７】

（１）コンテンツサーバ１００１にて、コンテンツを暗号化する場合、コンテンツの情報全てを暗号化しているが、これに限定されない。コンテンツの一部のみを暗号化してもよい。

（２）暗号化コンテンツの複製を鍵配信システム１０００を構成する再生装置１００４、記録媒体１００２、コンテンツサーバ１００１に対してのみ複製を許可するようにしてもよい。

【０２２８】

この場合、複製時に、複製元と複製先にて認証を行い、認証が成功した場合に複製を行うようにすればよい。

（３）または、認証が失敗する、つまり、共有秘密情報を有していない再生装置及び記録媒体に対しては、複製できる数を設定し、コンテンツサーバからのみ複製を許可するよ

うにしてもよい。このとき、複製が行われる度に複製できる数を１ずつ減算する。

【０２２９】

（４）記録媒体は、認証機能を備え、再生装置に装着されることにより利用されるＩＣ内蔵の可搬型記録媒体であればよい。例えば、ＳＤカードである。

または、ＩＣを備えていない可搬型記録媒体を利用する場合には、相互認証を行わないで、コンテンツサーバ１００１からの認証のみを行うようにしてもよい。

このとき、ＩＣを備えていない可搬型記録媒体に、共通秘密情報を記憶させておき、コンテンツサーバ１００１は、共通秘密情報が存在するか否かの判断による認証を行う。

【０２３０】

ＩＣを備えていない可搬型記録媒体は、例えば、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、ＤＶＤである。

または、記録媒体は、可搬型の記録媒体に限らず、携帯用の端末装置であってもよい。このとき、携帯用に端末装置は、ＧＷ１００７に接続され、コンテンツサーバ１００１へ利用種別が記録媒体である第３要求情報を送信し、認証が成功且つ配信可能なコンテンツ鍵の残数がある場合には、コンテンツサーバ１００１から暗号化された第２鍵情報を受信することができる。携帯用の端末装置とは、例えば、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　ＡＳＳｉＳｔａｎｔＳ）や、ノート型のパーソナルコンピュータである。

【０２３１】

（５）再生装置１００３に利用鍵確認部１２０３を設けたが、これに限定されない。利用鍵確認部１２０３を記録媒体１００２に備えて、再生装置１００３の時計部１２０６、通信部１２０５を用いて、機能を実現してもよい。

また、コンテンツサーバ１００１に設けた利用鍵確認部１０１９を、記録媒体１００２に備えてもよい。

【０２３２】

また、コンテンツサーバ１００１に設けた利用鍵事前配信部１０２０を、記録媒体１００２に備えてもよい。

（６）コンテンツサーバ１００１より配信するコンテンツ鍵の総数は、どのコンテンツ鍵に対しても同一の総数であったが、これに限定されない。コンテンツ鍵ごとに異なる総数としてもよい。この場合、コンテンツ取得部１０１５にて、入力部１０１６より総数を受け付け、受け付けた総数を用いて、コンテンツ鍵情報を生成し、生成したコンテンツ鍵情報を鍵情報記憶部１０３１へ記憶する。

【０２３３】

また、コンテンツ鍵情報の制限時間についても同様に、コンテンツ鍵ごとに異なる制限時間としてもよい。この場合、コンテンツ取得部１０１５にて、入力部１０１６より制限時間を受け付け、受け付けた制限時間を用いて、コンテンツ鍵情報を生成し、生成したコンテンツ鍵情報を鍵情報記憶部１０３１へ記憶する。

（７）コンテンツサーバ１００１より配信するコンテンツ鍵の総数を再生装置へ配信する数と記録媒体へ配信する数とを分けて管理してもよい。

【０２３４】

（８）再生装置１００３と再生装置１００４とを同一の再生装置としてもよい。

（９）記録媒体１００２をコンテンツサーバ１００１に装着した場合に、鍵の事前配信を可能としたが、再生装置１００３に装着した場合にも、コンテンツサーバ１００１からの鍵の事前配信を行えるようにしてもよい。

（１０）鍵情報テーブルＴ１００１と配信鍵情報テーブルＴ１００２とが分かれていたが、これらは、同一のテーブルで情報テーブルとしてもよい。

【０２３５】

このとき、情報テーブルは、コンテンツ鍵ＩＤ、コンテンツ鍵、対応情報ＩＤ、総数、残数、制限時間及び期限情報からなる組を１個以上記憶するための領域を備える。期限情報は、利用期限〔１〕、利用期限〔２〕、・・・、利用期限〔ｎ〕から構成構成される。ここで、「ｎ」は、総数に記録されている数以上の数である。利用期限〔１〕は、上記の

鍵配信方法の変形例で示した利用期限と同様の情報である。また、利用期限〔２〕、・・・、利用期限〔ｎ〕については、利用期限〔１〕と同様であるため、説明は省略する。

【０２３６】

（１１）再生装置１００３において、再生装置１００４と同様に、利用鍵監視部を備えてもよい。

このとき、再生装置１００３の利用鍵監視部は、記録媒体１００２に記憶された暗号化コンテンツの利用が終了したことを検知すると、暗号化コンテンツの利用に用いた第２鍵情報を削除し、鍵利用終了情報と、利用したコンテンツ鍵ＩＤと、コンテンツＩＤに対応する利用期限とからなる情報をコンテンツサーバ１００１へ送信する。

【０２３７】

コンテンツサーバ１００１は、再生装置１００３より上記情報を受信すると、鍵利用終了情報に含まれる情報ＩＤに対応するコンテンツ鍵情報の残数に１加算して、鍵情報テーブルＴ１００１の更新を行う。また、コンテンツサーバ１００１は、利用したコンテンツ鍵ＩＤと、コンテンツＩＤに対応する利用期限との組に対応する情報を配信鍵情報テーブルＴ１００２から削除する。

【０２３８】

（１２）記録媒体１００２に第２鍵情報を配信した場合、コンテンツサーバ１００１にて配信した第２鍵情報に含まれるコンテンツ鍵の利用期限を管理したが、再生装置１００４へ配信したコンテンツ鍵の利用期限も管理してもよい。

このとき、コンテンツサーバ１００１は、再生装置１００４へ第２鍵情報を送信し、再生装置１００４へ配信したコンテンツ鍵ＩＤと利用期限とからなる組を配信鍵情報テーブルＴ１００２へ記憶する。第２鍵情報の送信後は、時間管理部１０２３にて、利用期限の管理を行う。

【０２３９】

再生装置１００４では、記録媒体１００２に記憶された暗号化コンテンツの利用する場合と同様に、再生情報の受け付け後、受け付けた再生情報に含まれる情報ＩＤに対応するコンテンツ鍵が存在するか否かの判断を行い、コンテンツ鍵が存在すると判断する場合には、利用期限が過ぎているか否かの判断を行う。利用期限が過ぎていると判断する場合には、当該コンテンツ鍵を含むコンテンツ鍵管理情報を消去し、利用不可情報を利用者へ通知する。利用期限内であると判断する場合には、当該コンテンツ鍵を利用して、コンテンツを生成し、再生する。

【０２４０】

コンテンツ鍵が存在しないと判断する場合には、再生装置を示す情報が記録された利用種別と、受け取った再生情報に含まれる情報ＩＤとを含む第３要求情報を生成し、コンテンツサーバ１００１へ送信する。以降の動作は、鍵配信方法の変形例と同様であるため、説明は省略する。

また、コンテンツサーバ１００１の利用鍵記憶部１０１３へコンテンツ鍵を出力した場合にも、上記と同様の方法で、出力したコンテンツ鍵の利用期限を管理することができる。

【０２４１】

なお、配信される第２鍵情報は、上記の鍵配信方法の変形例と同様に暗号化されている。

（１３）または、再生装置１００４は、配信された第２鍵情報の管理を、コンテンツサーバ１００１と同様の方法で管理してもよい。

このとき再生装置１００４に時計部１３１０及び時間管理部１３１１を設ける。時計部１３１０は日時を計時する。時間管理部１３１１は、時計部１３１０にて計時される日時を用いて、利用鍵記憶部１３０２に記憶している第２鍵情報の利用期限が過ぎているか否かの判断を行う。利用期限が過ぎていると判断する場合には、当該第２鍵情報を消去し、鍵利用終了情報をコンテンツサーバ１００１へ送信する。

【０２４２】

また、コンテンツサーバ１００１においても、時計部１０２６、時間管理部１０２３及び利用鍵記憶部１０１３とを用いて、上記と同様の管理が可能である。

また、記録媒体１００２に時間管理部１１１０を設けて、上記と同様の管理を行ってもよい。この場合、上記にて示した動作は、再生装置１００３に装着され、電力が供給されている間のみ行われる。

【０２４３】

（１４）または、時間管理を行う再生装置と時間管理を行わない再生装置とを区別してもよい。なお、時間管理を行う再生装置には、記録媒体も含んでいる。

このとき、時間管理を行う再生装置は、利用種別の替わりに時間管理を行う再生装置であることを示す情報を付加した第３要求情報をコンテンツサーバ１００１へ送信し、時間管理を行わない再生装置は、利用種別の替わりに時間管理を行わない再生装置であることを示す情報を付加した第３要求情報をコンテンツサーバ１００１へ送信する。コンテンツサーバ１００１では、受信した第３要求情報を用いて、配信先の装置が、時間管理を行う再生装置であるか否かを判断し、時間管理を行う装置であると判断する場合には、暗号化された第２鍵情報を送信し、時間管理を行わない再生装置であると判断する場合には、暗号化された第１鍵情報を送信する。

【０２４４】

（１５）または、コンテンツサーバ１００１のみで再生装置１００４へ配信した第２鍵情報を管理してもよい。なお、第２鍵情報は、暗号化されて配信される。

このとき、再生装置１００４は、装置ＩＤを有している。ここで、装置ＩＤとは、再生装置を識別する識別子であり、再生装置ごとに、異なる装置ＩＤが割り当てられている。

コンテンツサーバ１００１は、配信したコンテンツ鍵と利用期限と配信した再生装置１００４の装置ＩＤとを記憶している。

【０２４５】

コンテンツサーバ１００１は、第２鍵情報を再生装置１００４へ送信した後、時間管理部１０２３にて、時計部１０２６で計時される日時を用いて、再生装置１００４へ配信したコンテンツ鍵の利用期限が過ぎているか否かを判断し、再生装置１００４へ配信したコンテンツ鍵の利用期限が過ぎたと判断する場合には、コンテンツサーバ１００１から、利用期限が過ぎたコンテンツ鍵ＩＤを含む鍵消去情報を、装置ＩＤに対応する再生装置１００４へ送信し、鍵情報テーブル内にて、該当するコンテンツ鍵情報に含まれる残数を１加算する。このとき、鍵消去情報を受信した再生装置１００４は、受信した情報に含まれるコンテンツ鍵ＩＤに対応する第２鍵情報を消去する。

【０２４６】

また、コンテンツサーバ１００１の利用鍵記憶部１０１３へコンテンツ鍵を出力した場合にも、上記と同様の方法で、管理することができる。

また、鍵配信システム１０００にて、再生装置１００４と同様の構成を備える再生装置が複数ある場合には、鍵消去情報を、少なくとも１台以上の再生装置へ一括送信してもよい。この場合、鍵情報テーブルＴ１００１内にて、該当するコンテンツ鍵情報に含まれる残数に加算される数は、鍵消去情報を送信した再生装置の数である。

【０２４７】

（１６）コンテンツサーバ１００１に、指定された時間に再生装置１００４へ第１鍵情報を配信する機能を備えてもよい。なお、配信される第１鍵情報は、上記の鍵配信方法の変形例と同様に暗号化されている。

このとき、コンテンツサーバ１００１は、さらに、コンテンツ鍵を配信する日時を示す配信日時と、配信する第１鍵情報と、配信する再生装置の装置ＩＤとからなる自動配信情報を記憶する自動配信情報記憶部１０４１と、第１鍵情報を配信する日時になったか否かを管理する自動配信管理部１０４２と、配信する日時になった場合に、第１鍵情報を配信する指定時間配信部１０４３を備えている。

【０２４８】

コンテンツサーバ１００１は、再生装置１００４より、コンテンツ鍵ＩＤと、自動配信

を行う日時情報と、端末ＩＤを含む自動要求情報を受け付けると、認証を行う。コンテンツサーバ１００１は、認証が成功した場合に、自動配信情報を生成し、生成した自動配信情報を自動配信情報記憶部１０４１へ記憶し、鍵情報テーブルＴ１００１内にて、該当するコンテンツ鍵情報に含まれる残数を１減算する。自動配信管理部１０４２は、時計部１０２６にて計時される日時を用いて、現在の日時が、自動配信情報記憶部１０４１に記憶している自動配信情報に含まれる配信日時になったか否かを判断し、配信日時になったと判断する場合に、指定時間配信部１０４３は、自動配信情報に含まれる装置ＩＤに対応する再生装置１００４へ第１鍵情報を配信し、自動配信情報記憶部１０４１に記憶している自動配信情報を消去する。

【０２４９】

なお、鍵配信システム１０００にて、再生装置１００４と同様の構成を備える再生装置が複数ある場合、それらの再生装置のうち少なくとも１台以上の再生装置より、同一の日時情報を受け付けた場合には、同一の日時を指定した各再生装置へ、コンテンツ鍵を一括配信してもよい。

また、自動配信情報記憶部１０４１に記憶する情報を、配信日時と、装置ＩＤと、第２鍵情報とし、再生装置１００４へは、上記に示した第１鍵情報の替わりに第２鍵情報を配信してもよい。

【０２５０】

また、記録媒体１００２に対しても指定された時間に第２鍵情報を配信してもよい。この場合、自動配信情報記憶部１０４１に記憶する装置ＩＤは、記録媒体１００２が装着された再生装置１００３の装置ＩＤである。

また、コンテンツサーバ１００１の入力部１０１６にて、自動要求情報を受け付けることにより、上記の動作と同様に、コンテンツサーバ１００１の利用鍵記憶部１０１３への自動配信も可能となる。ただし、認証は行わない。

【０２５１】

また、コンテンツサーバ１００１の入力部１０１６にて、コンテンツ鍵の配信先を記録媒体１００２又はコンテンツサーバ１００１の利用鍵記憶部１０１３の何れかを示す情報を付加した自動要求情報を受け付けることにより、コンテンツサーバ１００１の利用鍵記憶部１０１３への自動配信と記録媒体１００２への自動配信とを切り分けることができる。この場合、配信される情報は、第２鍵情報である。

【０２５２】

また、自動配信情報記憶部１０４１に記憶する情報を、配信日時と、装置ＩＤとし、自動配信時に、第１鍵情報又は第２鍵情報を生成してもよい。

また、自動配信される第１鍵情報は、共通鍵暗号により暗号化して送信してもよい。自動配信される第２鍵情報も同様である。

また、自動配信時に、再度認証を行ってもよい。この認証時に生成した暗号鍵を用いて、配信される第１鍵情報又は第２鍵情報を暗号化してもよい。

【０２５３】

（１７）鍵配信システム１０００において、配信されたコンテンツ鍵の配布先を検索する機能を追加してもよい。

このとき、再生装置１００４は、コンテンツサーバ１００１より指定されたコンテンツ鍵の存在を検索する鍵検索部１３２０を備え、また、記録媒体１００２も再生装置１００４と同様の鍵検索部１１２０を備える。

【０２５４】

コンテンツサーバ１００１は、検索したいコンテンツ鍵に対応するコンテンツ鍵ＩＤを含む鍵検索要求情報を同報通信的な方法により、再生装置１００３及び再生装置１００４へ送信する。

再生装置１００４は、コンテンツサーバ１００１より鍵検索要求情報を受信すると、鍵検索部１３２０にて、受信した鍵検索要求情報に含まれるコンテンツ鍵ＩＤが、利用鍵記憶部１３０２に存在する否かの判断を行い、存在すると判断する場合には、検索要求のあ

ったコンテンツ鍵を所有している旨の情報をコンテンツサーバ１００１へ送信する。

【０２５５】

再生装置１００３は、コンテンツサーバ１００１より鍵検索要求情報を受信すると、受信した鍵検索要求情報を記録媒体１００２へ出力する。記録媒体１００２は、鍵検索要求情報を受け取ると、鍵検索部１１２０にて、受け取った鍵検索要求情報に含まれるコンテンツ鍵ＩＤが、利用鍵記憶部１１０２に存在する否かの判断を行い、存在すると判断する場合には、検索要求のあったコンテンツ鍵を所有している旨の情報をコンテンツサーバ１００１へ送信する。

【０２５６】

また、コンテンツ鍵ＩＤを用いて、検索を行ったが、コンテンツ鍵ＩＤの替わりに、対応情報ＩＤを用いてもよい。この場合も、上記と同様の方法で、検索が可能である。

また、記録媒体１００２に鍵検索部１１２０を備える替わりに、再生装置１００３に鍵検索部を備えてもよい。

これにより、コンテンツ鍵を配信した再生装置及び記録媒体をデータベースなどによる管理を必要とせず、検索したいコンテンツ鍵を保有する再生装置及び記録媒体を管理することができる。

【０２５７】

（１８）コンテンツは、放送局から配信される情報としたが、これに限定されない。著作権の保護が必要な情報であればよい。

例えば、音楽情報、映像、プログラム等のデジタル化された情報である。

（１９）上記の鍵配信方法の変形例では、コンテンツサーバ１００１から再生装置１００４へ第１鍵情報を送信する際に、第１鍵情報に対応する暗号化コンテンツを送信してもよい。また、同様に、コンテンツサーバ１００１から記録媒体１００２へ第２鍵情報を送信する際に、第２鍵情報に対応する暗号化コンテンツを送信してもよい。

【０２５８】

（２０）記録媒体１００２に記録される第２鍵情報は、暗号化された第２鍵情報を記憶してもよい。

例えば、コンテンツサーバ１００１にて、第２鍵情報を生成後、共通秘密情報を暗号鍵として、第２鍵情報を暗号化し、暗号化した第２鍵情報（以下、「暗号化鍵情報」という。）を記録媒体１００２へ配信する。記録媒体１００２は、暗号化鍵情報を記憶し、利用時に共通秘密情報を用いて、暗号化鍵情報を復号して、第２鍵情報を生成して、生成した第２鍵情報を利用する。

【０２５９】

なお、暗号化鍵情報の配信時には、認証時に用いた共有秘密鍵を用いて暗号化して配信してもよい。

（２１）コンテンツサーバ１００１は、コンテンツサーバ１００１に装着された記録媒体１００２へコンテンツ鍵を出力する場合、出力する第２鍵情報を暗号化して出力したが、暗号化しないで出力してもよい。

【０２６０】

また、ネットワークを介して、再生装置１００４へ第１鍵情報を配信する場合や記録媒体１００２へ第２鍵情報を配信する場合も同様に、暗号化しないで配信してもよい。

（２２）配信されたコンテンツ鍵の利用回数を管理してもよい。

このとき、コンテンツ鍵を利用する度に、コンテンツ鍵の利用を示す情報をコンテンツサーバへ送信する。コンテンツサーバは、コンテンツ鍵の利用を示す情報を受け取ると、前記記録媒体へ配信したコンテンツ鍵の利用回数が、所定回数に達したか否かを判断し、所定回数に達した場合には、コンテンツ鍵に対応する残数に１加算し、記録媒体へ利用回数が所定回数に達した旨の情報を通知する。記録媒体は、利用回数が所定回数に達した旨の情報を受け取ると、コンテンツ鍵利用後、削除する。

【０２６１】

（２３）または、コンテンツサーバにて、記録媒体へ配信したコンテンツ鍵の利用状況

を示す履歴情報を管理し、ある所定期間以上利用されていなければ、前記コンテンツ鍵に対応する残数に１加算し、前記コンテンツ鍵の履歴情報に利用不可の情報を付加してもよい。

このとき、記録媒体は、配信されたコンテンツ鍵の利用を行う度に、コンテンツ鍵の利用を示す情報をコンテンツサーバへ送信する。コンテンツサーバは、コンテンツ鍵の利用を示す情報を受け取ると、記録媒体が利用するコンテンツ鍵が利用可能であるか否かを判断し、利用可能であれば、その情報を記憶する。利用可能でない場合には、利用不可を示す情報を記録媒体へ通知する。通知を受けた記録媒体は、コンテンツ鍵を削除する。

【０２６２】

また、コンテンツサーバでは、記憶された情報を用いて、最後にコンテンツ鍵を利用してから所定期間が過ぎたか否かを判断し、過ぎたと判断する場合に、前記コンテンツ鍵に対応する残数に１加算する。

（２４）上記の鍵配信方法の変形例にて示した利用鍵記憶部１０１３、利用鍵監視部１０１８、利用鍵確認部１０１９、利用鍵事前配信部１０２０、コンテンツ鍵制御部１０２１、認証部１０２２、時間管理部１０２３は、必ずしもコンテンツサーバ１００１内に含まれる必要はない。例えば、コンテンツサーバ１００１とは異なるネットワーク端末である鍵管理サーバを鍵配信システムの構成に追加し、鍵管理サーバ内に、利用鍵記憶部１０１３、利用鍵監視部１０１８、利用鍵確認部１０１９、利用鍵事前配信部１０２０、コンテンツ鍵制御部１０２１、認証部１０２２、時間管理部１０２３を備えてもよい。

【０２６３】

（２５）上記の鍵配信方法の変形例にて示したコンテンツ取得部１０１５は、放送局１００６より取得する暗号化されたコンテンツを復号する復号鍵を予め記憶しているが、これに限定されない。復号鍵は、暗号化されたコンテンツとともに、放送局１００６から配信されてもよい。

このとき、コンテンツ取得部１０１５は、放送局１００６より受信部１０１４を介して、暗号化されたコンテンツと復号鍵とを受信することとなる。

【０２６４】

（２６）上記の鍵配信方法の変形例にて示したコンテンツ取得部１０１５は、放送局１００６から取得した暗号化されたコンテンツを復号して、再度、コンテンツ鍵にて暗号化しているが、これに限定されない。暗号化されたコンテンツとその復号鍵とを、コンテンツ鍵にて暗号化して、暗号化コンテンツ情報を生成して、生成した暗号化コンテンツ情報を記憶してもよい。

【０２６５】

このとき、再生装置１００４及び記録媒体１００２へコンテンツを複製する場合には、情報ＩＤと、暗号化コンテンツ情報が複製される。再生装置１００４にて、コンテンツを利用する場合には、コンテンツサーバ１００１よりコンテンツ鍵を受け取ると、受け取ったコンテンツ鍵を用いて、暗号化コンテンツ情報を復号して、暗号化されたコンテンツと、その復号鍵とを生成して、生成した復号鍵を用いて、暗号化されたコンテンツを復号する。また、再生装置１００３にて、記録媒体１００２に記録されているコンテンツを利用する場合も同様の動作にて、暗号化されたコンテンツを復号する。

【０２６６】

（２７）上記鍵配信方法の変形例及び上記変形例をそれぞれ組み合わせるとしてもよい。

４．　ＡＤ内サーバに係る変形例

前記ＡＤ内サーバ１００は、コンテンツの複製に関し、グループ内装置に対して複製を許可するための管理情報と、グループ外の装置に対して複製を許可するための管理情報とを管理してもよい。

【０２６７】

以下に、前記ＡＤ内サーバが、前記グループ内及びグループ外装置それぞれに対する管理情報を保持する場合について説明する。

コンテンツの再生装置と、ホームサーバとの間のグループ登録手順、脱退手順については、前記した手順で行うものとし説明は省略する。

以下の説明では、グループ形成管理システムをコンテンツ複製管理システムと称し、前記ＡＤ内サーバをホームサーバと称する。

４．１　概要

図３６は、コンテンツ複製管理システム２０００の構成を示すブロック図である。

【０２６８】

ホームサーバ２００１と、再生装置２００２と、再生装置２００３とは、ゲートウェイ２００５を介して接続し、家庭内ネットワークを形成する。

記憶媒体２００４は、再生装置２００３が備える挿入口に挿入されることにより、再生装置２００３と接続する。

家庭内ネットワークにおいて、ホームサーバ２００１と、再生装置２００２と、再生装置２００３とは、それぞれＴＣＰ／ＩＰを用いて通信を行う。

【０２６９】

ゲートウェイ２００５が前記家庭内ネットワークと、外部ネットワークとの間のルーティング処理を行う。

再生装置２００６と、放送局２００７とは、前記外部ネットワークに接続する。

放送局２００７は、地上波デジタル放送を行う放送局であり、ＵＨＦ帯の電波を用いて、番組を各家庭に向けて放送する。

【０２７０】

ホームサーバ２００１は、地上波デジタル放送受信機能を備え、放送局２００７の放送内容を受信し、前記放送内容を所定の形式のデジタルデータに加工し、コンテンツとして大容量ハードディスクに蓄積する。

ホームサーバ２００１は、再生装置２００２、再生装置２００３、再生装置２００６に対する前記コンテンツの複製管理を行う。

【０２７１】

再生装置２００２、再生装置２００３、再生装置２００６は、ホームサーバ２００１から前記コンテンツの複製許可を受けた場合に、前記コンテンツをホームサーバ２００１から取得して記憶し、再生を行う。

本変形例では、家庭内ネットワークの範囲内をグループ２０１０とする。

グループ内においては、前記コンテンツの複製に関する制限が緩和される。

【０２７２】

グループ２０１０には、ホームサーバ２００１、再生装置２００２、再生装置２００３、ゲートウェイ２００５、記憶媒体２００４が属している。

前記外部ネットワークに属する装置は、家庭内ネットワーク或いはグループ２０１０の管理者が、管理出来ない装置である。

ホームサーバ２００１は、外部ネットワークに属する装置へ前記コンテンツを複製する場合、グループ２０１０内の装置への複製よりも、厳しい制限を行う必要がある。

【０２７３】

ホームサーバ２００１は、前記コンテンツの複製を許可する数により、前記制限を行う。

ホームサーバ２００１は、前記コンテンツの複製を許可する上限数を、グループ２０１０内と、家庭内ネットワークの範囲外であるグループ外とで分けて管理する。

グループ２０１０に属する装置や記憶媒体は、グループ２０１０に属していることを示す共通の情報であるグループ所属情報を、それぞれ保持する。

【０２７４】

前記グループ所属情報は、秘匿的に各装置、記憶媒体に配布された共通秘密情報、第三者である認証機関が発行したグループを構成する機器の機器リストから成る。

４．２　構成

４．２．１　ホームサーバ２００１

ホームサーバ２００１は、具体的には、ネットワーク通信機能と、大容量記憶領域を持つハードディスクとを備えるＤＶＤプレーヤー等である。

【０２７５】

図３７は、ホームサーバ２００１の構成を示すブロック図である。

通信部２１０１は、ネットワークを介して、他の装置とＴＣＰ／ＩＰによる通信を行う。

複製制限情報管理部２１０２は、コンテンツの複製に係る制御を行う。

図３８は、複製制限情報管理部２１０２が保持する情報を示す。

【０２７６】

図３８（α）は、複製制限情報管理部２１０２が保持する複製制限情報を示す。

前記複製制限情報は、コンテンツに対応づけられた情報であり、コンテンツ識別子と、グループ内装置残数と、グループ外装置残数と、グループ内媒体残数と、グループ外媒体残数と、使用期限情報とから成る。

前記複製制限情報は、放送局２００７から放送により取得するコンテンツに関する情報であり、放送局２００７から送信される放送とは別に、ネットワークを通じて放送局２００７から取得する。

【０２７７】

前記コンテンツ識別子は、各コンテンツに割り当てられたコンテンツを一意に識別する識別子である。

グループ内装置残数は、前記グループ内の装置に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

前記グループ内の装置に、前記コンテンツを複製した場合、複製制限情報管理部２１０２は、前記グループ内装置残数を１減少させる。

【０２７８】

前記グループ内の装置が、複製した前記コンテンツを消去した場合、複製制限情報管理部２１０２は、前記グループ内装置残数を１増加させる。

グループ外装置残数は、グループ外の装置に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

前記グループ外の装置に、前記コンテンツを複製した場合、複製制限情報管理部２１０２は、前記グループ外装置残数を１減少させる。

【０２７９】

前記グループ外の装置が、複製した前記コンテンツを消去した場合であっても、複製制限情報管理部２１０２は、前記グループ内装置残数を１増加させない。

前記グループ内媒体残数は、グループ内の記憶媒体に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

前記グループ外媒体残数は、グループ外の記憶媒体に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

【０２８０】

例えば、グループ２０１０内の再生装置２００２がサーバ２００１に対しコンテンツの複製を要求する場合、複製制限情報管理部２１０２は、グループ内装置残数が１以上である場合、前記要求に対し許可を与え、グループ内装置残数が０である場合は、前記要求に対し却下を通知する。

ホームサーバ２００１から再生装置２００２にコンテンツを複製する場合、複製制限情報管理部２１０２は、グループ内装置残数を１減少させる。

【０２８１】

また、再生装置２００２が、複製したコンテンツの消去をサーバ２００１に通知した場合、複製制限情報管理部２１０２は、グループ内装置複製残数を１増加させる。

前記使用期限情報は、前記コンテンツの使用可能な期限を示す情報である。

例えば、前記使用期限情報は、２００５年６月３０日といった具体的な日時を示す。

複製制限情報管理部２１０２は、前記使用期限情報が定められてコンテンツを複製した

場合、前記使用期限情報を時刻管理部２１０５が備えるタイマーに通知し、前記使用期限情報が示す時刻に、使用期限到達通知を出力するよう指示する。

【０２８２】

複製制限情報管理部２１０２は、時刻管理部２１０５から前記使用期限到達通知を取得した場合に、前記複製したコンテンツの使用が終了すると判定し、グループ内装置複製残数を１増加させる。

使用期限管理処理については、後述する。

複製制限情報管理部２１０２は、コンテンツの複製を要求する要求装置から、前記要求装置が複製を希望するコンテンツを識別するコンテンツ確認情報を含むコンテンツ確認要求を、ブロードキャストにより受信する。

【０２８３】

前記ブロードキャストを受信した場合、複製制限情報管理部２１０２は、通信部２１０１を介して、前記コンテンツ確認情報と一致するコンテンツ識別子を含む複製制限情報を管理しているか否かを確認し、保持している場合、ブロードキャストの送信元装置に対し、複製可を示す複製可否通知を送信する。

また、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）エコーメッセージを受信した場合、複製制限情報管理部２１０２は、ＩＣＭＰエコーリプライメッセージを送信元装置に対し送信する。

【０２８４】

複製制限情報管理部２１０２は、コンテンツ複製を要求する要求装置から、複製を希望するコンテンツを識別する前記コンテンツ確認情報と、記憶媒体が装置かの区分を示す装置属性情報を含むコンテンツ複製要求を受信し、認証部２１０３に対し認証開始指示を送信する。

複製制限情報管理部２１０２は、前記コンテンツ複製要求に基づき要求管理情報を生成する。

【０２８５】

前記要求管理情報は、複製か消去かの区別を示す処理区分と、コンテンツを識別する前記コンテンツ確認情報と、前記要求装置のＩＰアドレスと、前記要求装置がグループ内かグループ外かを示す前記グループ内外情報と、要求装置が媒体か装置のいずれかを示す装置属性情報と、予約情報と、次の要求管理情報を保持している場所を示す次要求ポインタとから成る。

【０２８６】

前記予約情報は、前記コンテンツの複製或いは消去を開始する時刻を示す。

例えば、前記予約情報は、２００５年６月３０日といった具体的な日時を示す。

複製制限情報管理部２１０２は、コンテンツの複製を要求する要求装置から、前記予約情報をコンテンツの複製予約要求と共に取得する。

図３８（ｂ）は、前記要求管理情報をキューを用いて管理する要求管理キューを示す図である。

【０２８７】

図３８（ｂ）では、前記要求管理キューに、前記要求管理情報が３つ繋がっている例を示している。

複製制限情報管理部２１０２は、前記コンテンツ複製要求を受信した場合、前記コンテンツ複製要求に含まれるコンテンツ確認情報と、前記装置属性情報と、要求装置のＩＰアドレスとを生成した前記要求管理情報に書き込む。

【０２８８】

複製制限情報管理部２１０２は、認証部２１０３から前記グループ内外情報を取得して、前記要求管理情報に書き込む。

ホームサーバ２００１は、要求先頭ポインタが指す要求管理情報が示す要求から順に、対応する処理を行う。

前記対応する処理が終わると、複製制限情報管理部２１０２は、前記要求先頭ポインタ

の内容を、前記要求管理情報内の次要求ポインタが示す要求管理情報を指すように書き換える。

【０２８９】

また、新たな要求を他装置から取得した場合、複製制限情報管理部２１０２は、取得した要求に応じた要求管理情報を新たに作成し、キューの最後に繋ぐ。

前記要求管理情報中の前記処理区分が、複製を示す場合、前記要求管理情報中の前記グループ内外情報と、前記装置属性情報との組み合わせに基づき、処理の対象となる対象残数をグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ内媒体残数から１つ選択する。

【０２９０】

例えば、前記グループ内外情報がグループ内を示し、前記装置属性情報が装置を示す場合、前記対象残数は、グループ内装置残数となり、前記グループ内外情報がグループ内を示し、前記装置属性情報が媒体を示す場合、前記対象残数は、グループ内媒体残数となる。

次に、前記要求管理情報中のコンテンツ確認情報に一致するコンテンツ識別子を持つ複製制限管理情報中の、前記対象残数が０か否かを調べる。

【０２９１】

複製制限情報管理部２１０２は、前記対象残数が０でない場合、前記コンテンツ識別子で識別されるコンテンツが、複製可であると判定し、０であった場合は、複製不可と判定する。

複製可であった場合、前記コンテンツを暗号化し、前記要求装置に送信するよう、暗号復号化部２１０４に指示する。

【０２９２】

暗号復号化部２１０４は、前記指示に従い前記コンテンツを暗号化し、前記要求装置に送信する。

前記要求管理情報中の前記処理区分が、消去を示す場合、複製制限情報管理部２１０２は、前記要求管理情報中の前記グループ内外情報と、前記装置属性情報との組み合わせに基づき、処理の対象となる対象残数をグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ内媒体残数から１つ選択する。

【０２９３】

複製制限情報管理部２１０２は、前記要求装置に対し、返却処理開始通知を送信する。

また、複製制限情報管理部２１０２は、前記要求装置から、コンテンツ消去完了通知を受信した場合、前記要求管理情報中のコンテンツ確認情報に一致するコンテンツ識別子を持つ複製制限管理情報中の、前記対象残数を１増加させる。

複製制限情報管理部２１０２は、キュー先頭の前記要求管理情報を削除し、前記要求管理キューを更新する。

【０２９４】

また、複製制限情報管理部２１０２は、要求装置から、複製制限管理情報の譲渡要求を受信する。

複製制限情報管理部２１０２は、管理している前記複製制限管理情報の一部或いは全てを他の装置に譲渡する処理を行う。

複製制限管理情報譲渡処理については、後述する。

【０２９５】

複製制限情報管理部２１０２は、コンテンツの複製を要求する要求装置から、通信部２１０１を介して、複製予約要求を受信する。

前記複製予約要求は、複製要求に係るコンテンツを示すコンテンツ情報と、コンテンツの複製を開始する時刻を示す前記予約情報とを含む。

複製制限情報管理部２１０２は、前記複製予約要求を受信した場合、前記複製予約要求に含まれる前記コンテンツ指定情報に一致する前記コンテンツ識別子を保持しているか判定し、保持している場合は、前記複製開始時刻情報を前記コンテンツ識別子に対応づけて

保持する。

【０２９６】

また、時刻管理部２１０５が備えるタイマーに対し、前記複製開始時刻情報を通知し、前記複製開始時刻情報が示す時刻に、予約時刻到達通知を出力するよう指示する。

複製制限情報管理部２１０２は、前記予約時刻到達通知を取得した場合、前記コンテンツの複製を実行する。

予約管理処理ついては、後述する。

【０２９７】

認証部２１０３は、複製制限情報管理部２１０２から、前記認証開始指示を受信し、コンテンツの複製を要求する要求装置との間で、相互認証と鍵共有を実行する。

また、認証部２１０３は、グループ２０１０に属していることを示す情報であるグループ所属情報を保持する。

前記グループ所属情報は、秘匿的に各装置、記憶媒体に配布された共通秘密情報、第三者である認証機関が発行したグループを構成する機器の機器リストから成る。

【０２９８】

前記相互認証と鍵共有については、後述する。

前記相互認証と鍵共有が成功した場合には、認証部２１０３と、前記要求装置とは、同一の鍵であるセッション鍵を共有する。

認証部２１０３は、前記セッション鍵を保持し、かつ、暗号復号化部２１０４に前記セッション鍵を通知する。

【０２９９】

また認証部２１０３は、要求装置から、グループ所属情報を受信する。

前記受信したグループ所属情報と、保持しているグループ所属情報とが一致するか否かを判定し、一致する場合グループ内を示す、一致しない場合グループ外を示すグループ内外情報を、複製制限情報管理部２１０２に通知する。

暗号復号化部２１０４は、認証部２１０３が行う前記相互認証と鍵共有が成功した後、認証部２１０３から前記セッション鍵を取得する。

【０３００】

暗号復号化部２１０４は、前記相互認証と鍵共有が成功した後に、前記要求装置へ送信するデータの暗号化、前記要求装置から受信したデータの復号化を、前記セッション鍵を用いて行う。

時間管理部２１０５は、時計と、タイマーを備える。

前記時計は、例えば、１秒毎にカウントアップし、１９７０年１月１日０時０分０秒からの秒数を示すカウンタで構成する。

【０３０１】

前記タイマーには、通知要求元から、タイマー通知要求時刻が設定される。

前記タイマーは、前記時計が、前記タイマー通知要求時刻で示される時刻を指したとき、前記通知要求元に対し、設定した時刻に到達したことを示す通知を行う。

地上波デジタル放送受信部２１０６は、放送局２００７から番組を受信する。

地上波デジタル放送受信部２１０６は、受信した放送波に対し、規定の方法により復調、多重分離、復号等を行うことにより、映像情報、音声情報、データ放送用情報、コンテンツ識別子を含むその他コンテンツ再生に必要な制御情報等を取得する。

【０３０２】

地上波デジタル放送受信部２１０６は、前記映像情報、音声情報及びデータ放送用情報を、パーシャルＴＳ等の所定の形式のデジタルデータに変換し、記憶部２１０７にコンテンツとして出力する。

記憶部２１０７は、地上波デジタル放送受信部２１０６から受信した前記コンテンツを、前記コンテンツ識別子と対応づけて蓄積する。

【０３０３】

記憶部２１０７は、耐タンパ機能を有し、保持する情報を、装置外部から知られること

はない。

４．２．２　再生装置２００２

再生装置２００２は、具体的には、ネットワーク通信機能と、大容量記憶領域を持つハードディスクとを備えるＤＶＤプレーヤー等である。

【０３０４】

図３９は、再生装置２００２の構成を示すブロック図である。

通信部２２０１は、ネットワークを介して、他の装置とＴＣＰ／ＩＰによる通信を行う。

複製制限情報管理部２２０２は、コンテンツの複製管理を行う。

複製制限情報管理部２２０２の動作は、複製制限情報管理部２１０２とほぼ同じであるので、異なる動作について説明する。

【０３０５】

複製制限情報管理部２２０２は、コンテンツの複製元装置に対し、複製を希望するコンテンツを識別する前記コンテンツ確認情報と、記憶媒体か装置かの区分を示す装置属性情報を含むコンテンツ複製要求を送信する。

前記装置属性情報は、コンテンツの複製要求を行う主体が、再生装置２００２のような装置の場合は装置を示し、ＩＣ内蔵可搬型記憶媒体２００４のように記憶媒体の場合は媒体を示す情報である。

【０３０６】

よって、再生装置２００２が送信する前記装置属性情報は、装置を示す。

複製制限情報は、コンテンツの配布を行うサーバが管理する。

再生装置２００２は、コンテンツの複製を許可する権限を持つホームサーバ２００１から、前記複製を許可する権限の譲渡を受けることにより、コンテンツを配布する権限を持つこととなる。

【０３０７】

複製制限情報管理部２２０２は、ホームサーバ２００１から、前記コンテンツ識別子と、前記グループ内装置残数と、前記グループ外装置残数と、前記グループ内媒体残数と、前記グループ外媒体残数と、前記使用期限情報とを取得し、前記複製制限情報として保持する。

前記複製を許可する権限の譲渡を受けた複製制限情報管理部２２０２は、複製制限情報管理部２１０２と同じ構成である。

【０３０８】

ここで、再生装置２００２は、取得した前記コンテンツ識別子に対応するコンテンツを保持する必要はなく、他の装置が、前記コンテンツ識別子に対応するコンテンツを保持していてもよい。

この場合、他の装置から前記コンテンツの複製の要求を受け、前記コンテンツの複製を許可する場合、前記コンテンツを保持している装置に対し、前記コンテンツを、前記複製要求を行った装置に対し送信するよう指示する。

【０３０９】

また、ホームサーバ２００１から取得する前記グループ内装置残数と、前記グループ外装置残数と、前記グループ内媒体残数と、前記グループ外媒体残数とは、前記ホームサーバ２００１が保持する残数の全てではなく一部でもよい。

例えば、ホームサーバ２００１は、前記グループ内装置残数として値「１０」を保持している場合に、再生装置２００２に対し、前記グループ内装置残数として値「５」だけ譲渡してもよい。

【０３１０】

上記の場合、再生装置２００２は、グループ内の装置に対し、前記コンテンツを５つまで、複製許可する権限を持つ。

また、再生装置２００２は、ホームサーバ２００１から取得した前記複製制限情報の一部或いは全てを返却してもよい。

再生装置２００２は、ホームサーバ２００１に対し、前記グループ内装置残数として値「２」だけ返却してもよい。

【０３１１】

前記複製制限情報の譲渡と返却については後述する。

認証部２２０３は、認証相手である認証装置と、相互認証と鍵共有を実行する。

認証部２２０３は、グループ２０１０に属していることを示す情報である前記グループ所属情報を保持する。

前記相互認証と鍵共有については、後述する。

【０３１２】

前記相互認証と鍵共有が成功した場合には、認証部２２０３と、前記認証装置とは、同一の鍵であるセッション鍵を共有する。

認証部２２０３は、前記セッション鍵を保持し、かつ、暗号復号化部２２０４に前記セッション鍵を通知する。

暗号復号化部２２０４は、認証部２２０３が行う前記相互認証と鍵共有が成功した後、認証部２２０３から前記セッション鍵を取得する。

【０３１３】

暗号復号化部２２０４は、前記相互認証と鍵共有が成功した後に、前記認証装置へ送信するデータの暗号化、前記認証装置から受信したデータの復号化を、前記セッション鍵を用いて行う。

時間管理部２２０５は、時計と、タイマーを備える。

前記時計は、例えば、１秒毎にカウントアップし、１９７０年１月１日０時０分からの秒数を示すカウンタで構成する。

【０３１４】

前記タイマーには、通知要求元から、タイマー通知要求時刻が設定される。

前記タイマーは、前記時計が、前記タイマー通知要求時刻で示される時刻を指したとき、前記通知要求元に対し、設定した時刻に到達したことを示す通知を行う。

コンテンツ配布元決定部２２０６は、サーバ或いはコンテンツの複製権を譲渡された装置の中から、コンテンツの複製許可を受ける装置である配布元装置を決定する。

【０３１５】

コンテンツ配布元決定部２２０６は、ネットワーク上に、複製を希望するコンテンツを示すコンテンツ識別情報を含むコンテンツ確認情報をブロードキャストをする。

コンテンツ配布元決定部２２０６は、前記コンテンツ確認情報に応答してきた装置に対し、順番に、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）エコーメッセージを送信し、前記送信時から、応答であるＩＣＭＰエコーリプライメッセージを受信するまでの応答時間を測定していく。

【０３１６】

コンテンツ配布元決定部２２０６は、応答時間が最短であった装置を配布元装置に決定し、前記配布元装置を、複製制限情報管理部２２０２に通知する。

記憶部２２０７は、コンテンツの保持を行う。

再生部２２０８は、記憶部２２０７に保持しているコンテンツ、或いは通信部２２０１が受信したコンテンツの再生を行う。

４．２．３　再生装置２００３

再生装置２００３は、具体的には、ネットワーク通信機能を備えたＳＤプレーヤーである。

【０３１７】

図４０は、再生装置２００３とＩＣ内蔵可搬型記憶媒体２００４との構成を示すブロック図である。

通信部２３０１は、ネットワークを介して、他の装置とＴＣＰ／ＩＰによる通信を行う

通信部２３０３は、ＩＣ内蔵可搬型記憶媒体と接続し、通信を行う。

【０３１８】
再生部２３０２は、ＩＣ内蔵可搬型記憶媒体から読み出すコンテンツを再生する。
４．２．４　ＩＣ内蔵可搬型記憶媒体２００４
ＩＣ内蔵可搬型記憶媒体２００４は、具体的には、ＩＣを内蔵する、耐タンパ性を有したＳＤカードである。
入出力部２３１１は、再生装置２００３との通信を行う。
【０３１９】
ＩＣ内蔵可搬型記憶媒体２００４は、再生装置２００３を介して、他の装置と通信を行う。
コンテンツ配布元決定部２３１２の説明は、前述したコンテンツ配布元決定部２２０６と同じ説明となる。
コンテンツ配布元決定部２３１２は、決定した配布元装置に対し、コンテンツ識別情報を含むコンテンツ複製要求を送信する。
【０３２０】
認証部２３１３は、認証を行う相手である認証装置と、再生装置２００３及びネットワークを介して通信を行い、相互認証と鍵共有を実行する。
認証部２３１３は、グループ２０１０に属していることを示す情報である前記グループ所属情報を保持する。
相互認証と鍵共有については後述する。
【０３２１】
前記相互認証と鍵共有が成功した場合には、認証部２３１３と、前記認証装置とは、同一の鍵であるセッション鍵を共有する。
認証部２３１３は、前記セッション鍵を保持し、かつ、暗号復号化部２３１４に前記セッション鍵を通知する。
暗号復号化部２３１４は、認証部２３１３が行う前記相互認証と鍵共有が成功した後、認証部２３１３から前記セッション鍵を取得する。
【０３２２】
暗号復号化部２３１４は、前記相互認証と鍵共有が成功した後に、前記認証装置へ送信するデータの暗号化、前記認証装置から受信したデータの復号化を、前記セッション鍵を用いて行う。
記憶部２３１５は、コンテンツの保持を行う。
４．２．５　再生装置２００６
再生装置２００６は、具体的には、ネットワーク通信機能、大容量のハードディスクを備えたＤＶＤプレーヤー等である。
【０３２３】
図４１は、再生装置２００６の構成を示すブロック図である。
通信部２４０１は、ネットワークを介して、他の装置とＴＣＰ／ＩＰによる通信を行う。
認証部２４０２は、コンテンツを保持するサーバとの間で、相互認証と鍵共有を実行する。
【０３２４】
但し、認証部２４０２は、前記グループ所属情報を保持しないため、ホームサーバ２００１において、再生装置２００６がグループ外の装置であると判定される。
前記相互認証と鍵共有については、後述する。
前記相互認証と鍵共有が成功した場合には、認証部２４０２と、前記サーバとは、同一の鍵であるセッション鍵を共有する。
【０３２５】
認証部２４０２は、前記セッション鍵を保持し、かつ、暗号復号化部２４０３に前記セッション鍵を通知する。
暗号復号化部２４０３は、認証部２４０２が行う前記相互認証と鍵共有が成功した後、

認証部２４０２から前記セッション鍵を取得する。
暗号復号化部２４０３は、前記相互認証と鍵共有が成功した後に、前記認証装置へ送信するデータの暗号化、前記認証装置から受信したデータの復号化を、前記セッション鍵を用いて行う。
【０３２６】
記憶部２４０４は、コンテンツの保持を行う。
４．３　動作
４．３．１　コンテンツ複製元決定処理
コンテンツの複製を要求する要求装置は、ネットワーク上の装置の中から、所望のコンテンツの複製元となる配信装置を決定する。
【０３２７】
図４２は、コンテンツ複製元決定処理を示すフローチャートである。
ここでは、要求装置は再生装置２００２であり、配信装置はホームサーバ２００１であり、他装置は再生装置２００３であるものとする。
前記配信装置は、コンテンツ複製元決定処理において結果的に、前記配信装置からコンテンツ複製元として選択された装置を示す。
【０３２８】
前記他装置は、コンテンツ複製元決定処理において、結果的に、前記配信装置からコンテンツ複製元として選択されなかった装置を示す。
前記要求装置は、コンテンツを要求する装置であり、再生装置２００３が、コンテンツの複製要求を行う場合であれば、再生装置２００３が前記要求装置となる。
前記要求装置は、所望のコンテンツ識別情報が示すコンテンツを、いずれの装置から複製してもらうかを決定する。
【０３２９】
前記要求装置は、所望のコンテンツを保持している装置から応答を取得する目的で、コンテンツ確認要求をネットワーク上にブロードキャスト送信する（Ｓ２００１）。
前記コンテンツ確認要求は、要求装置が複製を希望するコンテンツを識別するコンテンツ確認情報を含む。
前記配信装置及び前記他装置は、前記コンテンツ確認要求を受信する。
【０３３０】
前記配信装置は、前記コンテンツ確認要求中の前記コンテンツ確認情報と一致するコンテンツ識別子を管理しているか確認する（Ｓ２００２）。
前記他装置は、前記コンテンツ確認情報と一致するコンテンツ識別子を保持しているか確認する（Ｓ２００３）。
前記配信装置は、一致するコンテンツ識別子を管理している場合（Ｓ２００２：ＹＥＳ）、複製可を示す複製可否通知を要求装置へ送信する（Ｓ２００４）。
【０３３１】
前記配信装置は、一致するコンテンツ識別子を管理していない場合（Ｓ２００２：ＮＯ）、処理を終了する。
前記他装置は、一致するコンテンツ識別子を管理している場合（Ｓ２００３：ＹＥＳ）、複製可を示す複製可否通知を要求装置へ送信する（Ｓ２００５）。
前記他装置は、一致するコンテンツ識別子を管理していない場合（Ｓ２００３：ＮＯ）、処理を終了する。
【０３３２】
前記要求装置は、受信した各複製可否通知の内容を確認し、複製可を示す複製可否通知を送信した装置の送信元ＩＰアドレスを保持する（Ｓ２００６）。
前記要求装置は、前記保持したＩＰアドレスを持つ各装置に対し、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ　Ｐｒｏｔｏｃｏｌ）エコーメッセージを送信し、前記送信時から、応答であるＩＣＭＰエコーリプライメッセージを受信するまでの応答時間を測定する。

【０３３３】
前記要求装置は、前記配信装置に対し、ＩＣＭＰエコーメッセージを送信する（Ｓ２００７）。
前記配信装置は、ＩＣＭＰエコーメッセージを受信し、応答として前記要求装置に対し、ＩＣＭＰリプライメッセージを送信する（Ｓ２００８）。
前記要求装置は、ＩＣＭＰエコーリプライメッセージを受信し、測定した前記応答時間を保持する。
【０３３４】
前記要求装置は、前記他装置に対し、ＩＣＭＰエコーメッセージを送信する（Ｓ２００９）。
前記他装置は、ＩＣＭＰエコーメッセージを受信し、応答として前記要求装置に対し、ＩＣＭＰエコーリプライメッセージを送信する（Ｓ２０１０）。
前記要求装置は、ＩＣＭＰエコーリプライメッセージを受信し、測定した前記応答時間を保持する。
【０３３５】
前記要求装置は、複製元装置として、前記応答時間が最短であった装置を選択し、複製元装置のＩＰアドレスを保持しておく（Ｓ２０１１）。
４．３．２　相互認証と鍵共有
図４３及び図４４は、配信装置と要求装置との間で行われる相互の機器認証及び鍵共有の動作を示すフローチャートである。
【０３３６】
ここでは、再生装置２００２が、図４２に示したコンテンツ複製元決定処理により、複製元としてホームサーバ２００１を選択したものとする。
よって、配信装置はホームサーバ２００１であり、要求装置は再生装置２００２である例で説明する。
ホームサーバ２００１の認証部２１０３は、著作権保護ライセンサ（ＣＡ）の公開鍵ＰＫ－ＣＡ、秘密鍵ＳＫ－Ａ及び公開鍵証明書Ｃｅｒｔ－Ａを予め記憶しており、楕円曲線Ｅによる暗号処理部を有している。
【０３３７】
また、再生装置２００２の認証部２２０３は、著作権保護ライセンサの公開鍵ＰＫ－ＣＡ、秘密鍵ＳＫ－ｉ及び公開鍵証明書Ｃｅｒｔ－ｉを予め記憶しており、楕円曲線Ｅによる暗号処理部を有している。
また、Ｓｉｇ（ＳＫ、Ｄ）は、秘密鍵ＳＫを用いてデータＤにデジタル署名を施す演算である。
【０３３８】
また、Ｇは、楕円曲線Ｅ上のベースポイントであり、本認証システムに固有の値である。
また、「＊」は、楕円曲線Ｅ上の乗算を示す演算子である。
例えば、「ｘ＊Ｇ」は、楕円曲線Ｅ上の点Ｇをｘ個、加算する演算である。
「｜｜」は、結合を示す演算子であり、例えば、「Ａ｜｜Ｂ」は、「Ａ」と「Ｂ」との結合結果である。
【０３３９】
以下において、「認証部２１０３は、認証部２２０３へ情報を出力する」及び「認証部２２０３は、認証部２１０３へ情報を出力する」などは、簡略化した記載であり、それぞれ、「認証部２１０３は、通信部２１０１及び通信部２２０１を介して、認証部２２０３へ情報を出力する」及び「認証部２２０３は、通信部２２０１及び通信部２１０１を介して、認証部２１０３へ情報を出力する」を意味するものである。
【０３４０】
認証部２２０３は、乱数ｙを生成し（Ｓ２１０１）、生成した乱数ｙ及び公開鍵証明書Ｃｅｒｔ－ｉを認証部２１０３へ出力する（Ｓ２１０２）。

認証部２１０３は、乱数ｙ及び公開鍵証明書Ｃｅｒｔ－ｉを受け取り（Ｓ２１０２）、ＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ Ｒｅｖｏｃａｉｏｎ Ｌｉｓｔ）を用いて、再生装置２００２の公開鍵証明書Ｃｅｒｔ－ｉが無効化されていないかどうかを確認する（Ｓ２１０３）。

【０３４１】

無効化されている場合（Ｓ２１０４：ＮＯ）、処理を終了する。

無効化されていない場合（Ｓ２１０４：ＹＥＳ）、認証部２１０３は、公開鍵ＰＫ－ＣＡを用いて公開鍵証明書Ｃｅｒｔ－ｉの検証を行う（Ｓ２１０５）。

検証に失敗すると（Ｓ２１０６：ＮＯ）、認証部２１０３は、処理を終了する。

検証に成功すると（Ｓ２１０６：ＹＥＳ）、認証部２１０３は、乱数×を生成し（Ｓ２１０７）、生成した乱数×及び公開鍵証明書Ｃｅｒｔ－Ａを認証部２２０３へ出力する（Ｓ２１０８）。

【０３４２】

認証部２２０３は、認証部２１０３から乱数×及び公開鍵証明書Ｃｅｒｔ－Ａを受け取る（Ｓ２１０８）。

次に、認証部２２０３は、ＣＲＬを用いて、ホームサーバ２００１の公開鍵証明書Ｃｅｒｔ－Ａが無効化されていないかどうかを確認する（Ｓ２１０９）。

無効化されている場合（Ｓ２１１０：ＮＯ）、認証部２２０３は、処理を終了する。

【０３４３】

無効化されていない場合（Ｓ２１１０：ＹＥＳ）、認証部２２０３は、公開鍵ＰＫ－ＣＡを用いて公開鍵証明書Ｃｅｒｔ－Ａの検証を行う（Ｓ２１１１）。

検証に失敗すると（Ｓ２１１２：ＮＯ）、認証部２２０３は、処理を終了する。

検証に成功すると（Ｓ２１１２：ＹＥＳ）、認証部２２０３は、乱数ｙ’を生成し（Ｓ２１１３）、署名データＳ１＝Ｓｉｇ（ＳＫ－ｉ、（ｙ’＊Ｇ）｜｜×）を生成し（Ｓ２１１４）、ｙ’＊Ｇ及びＳ１を認証部２１０３へ出力する（Ｓ２１１５）。

【０３４４】

認証部２１０３は、認証部２２０３からｙ’＊Ｇ及びＳ１を受け取る（Ｓ２１１５）。

次に、認証部２１０３は、Ｓ１の検証を行う（Ｓ２１１６）。

検証に失敗した場合は（Ｓ２１１７）、認証部２１０３は、処理を終了する。

検証に成功した場合（Ｓ２１１７）、認証部２１０３は、乱数×’を生成し（Ｓ２１１８）、署名データＳ０＝Ｓｉｇ（ＳＫ－Ａ、（×’＊Ｇ）｜｜ｙ）を生成し（Ｓ２１１９）、×’＊Ｇ及びＳ０を認証部２２０３へ出力する（Ｓ２１２０）。

【０３４５】

認証部２２０３は、認証部２１０３から×’＊Ｇ及びＳ０を受け取り（Ｓ２１２０）、次に、認証部２２０３は、Ｓ０の検証を行う（Ｓ２１２１）。

検証に失敗すると（Ｓ２１２２：ＮＯ）、認証部２２０３は、処理を終了する。

検証に成功すると（Ｓ２１２２：ＹＥＳ）、認証部２２０３は、セッション鍵Ｋ’＝ｙ’（×’＊Ｇ）を算出する（Ｓ２１２４）。

【０３４６】

一方、認証部２１０３は、認証部２１０３は、セッション鍵Ｋ＝×’（ｙ’＊Ｇ）を算出する（Ｓ２１２３）。

以上のようにして、ホームサーバ２００１及び再生装置２００２の間の相互の機器認証と鍵共有とが行われる。

セッション鍵Ｋ及びＫ’は、それぞれホームサーバ２００１及び再生装置２００２において共有される同一の値を有する鍵である。

４．３．３　コンテンツ複製処理

図４５は、コンテンツの複製処理を示す図である。

【０３４７】

図４５中、要求装置が再生装置２００２であり、配信装置がホームサーバ２００１であり、他装置が再生装置２００３である場合を例として説明する。

前記配信装置と、前記要求装置と、前記他装置とは、図４２に示すコンテンツ複製元決定処理を行う（Ｓ２２０１）。

前記要求装置は、前記コンテンツ複製元決定処理により、複製元である配信装置としてホームサーバ２００１を選択したものとする。

【０３４８】

前記要求装置は、前記配信装置に対し、複製を希望するコンテンツを識別する前記コンテンツ確認情報と、記憶媒体か装置かの区分を示す前記装置属性情報を含むコンテンツ複製要求を送信する（Ｓ２２０２）。

前記配信装置は、前記コンテンツ複製要求を受信し、前記要求装置のＩＰアドレスと共に保持する。

【０３４９】

前記配信装置と、前記要求装置とは、図４３及び図４４に示した、相互認証と鍵共有を行う（Ｓ２２０３）。

前記配信装置と、前記要求装置とは、Ｓ２２０３の実行結果としてセッション鍵を共有する。

前記配信装置と前記要求装置とは、セッション鍵の共有が完了した以降の通信を、前記セッション鍵を用いて暗号化及び復号化する。

【０３５０】

前記要求装置は、前記グループ所属情報を、前記配信装置に送信する（Ｓ２２０４）。

前記要求装置は、受信した前記グループ所属情報と、認証部２１０３で保持しているグループ所属情報とが一致しているか否かを判定する（Ｓ２２０５）。

前記配信装置は、Ｓ２２０３において、相互認証と鍵共有が成功した場合、前記保持した前記コンテンツ複製要求と、ＩＰアドレスと、Ｓ２２０５における判定結果とに基づき前記要求管理情報を生成し前記管理要求キューに繋ぐ（Ｓ２２０６）。

【０３５１】

前記配信装置は、Ｓ２２０６において繋いだ前記要求管理情報がキューの先頭になるのを待つ（Ｓ２２０７）。

前記配信装置は、前記要求管理情報がキューの先頭になった場合、前記要求管理情報に基づきコンテンツの複製処理を再開する。

配信装置は、前記要求管理情報中のグループ内外情報と、前記装置属性情報とに基づき、対象残数を選択し、前記対象残数が０であるか否かを判定する（Ｓ２２０８）。

【０３５２】

前記対象残数は、グループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数から選択した１の残数である。

前記グループ内外情報がグループ内を示し、前記装置属性情報が装置を示す場合、前記対象残数はグループ内装置残数である。

同様に、前記グループ内外情報がグループ外を示し、前記装置属性情報が装置を示す場合、前記対象残数はグループ外装置残数である。

【０３５３】

前記グループ内外情報がグループ内を示し、前記装置属性情報が媒体を示す場合、前記対象残数はグループ内媒体残数である。

前記グループ内外情報がグループ外を示し、前記装置属性情報が媒体を示す場合、前記対象残数はグループ外媒体残数である。

前記対象残数が０である場合（Ｓ２２０８：ＹＥＳ）、前記配信装置は、複製不可を示す複製可否通知を、前記要求装置に送信し処理を終了する（Ｓ２２０９）。

【０３５４】

前記要求装置は、複製不可を示す複製可否通知を配信装置から受信したか否かを判定する（Ｓ２２１０）。

前記複製可否通知を受けたと判定した場合（Ｓ２２１０：ＹＥＳ）、要求装置は処理を終了する。

前記対象残数が０でない場合（Ｓ２２０８：ＮＯ）、前記配信装置は、コンテンツをセッション鍵で暗号化し（Ｓ２２１１）、配信装置へ送信する（Ｓ２２１２）。

【０３５５】

前記要求装置は、受信した前記暗号化されたコンテンツをセッション鍵を用いて復号化し、記憶部２２０７に保持する（Ｓ２２１３）。

前記要求装置は、前記配信装置に対し、コンテンツ複製完了通知を送信する（Ｓ２２１４）。

前記配信装置は、前記コンテンツ複製完了通知を受信し、前記対象残数を１減少させる（Ｓ２２１５）。

【０３５６】

配信装置は、前記要求管理キューの先頭の前記要求管理情報を削除し、前記要求管理キューを更新する（Ｓ２２１６）。

４．３．４　複製制限管理情報譲渡処理

前記配信装置が、管理している前記複製制限管理情報を他の装置に譲渡することにより、前記他の装置が前記コンテンツの複製を許可する権限を持つこととなる。

【０３５７】

図４６は、複製制限管理情報譲渡処理を示すフローチャートである。

ここでは、要求装置は再生装置２００２であり、配信装置はホームサーバ２００１であり、他装置は再生装置２００３であるものとする。

前記要求装置は、まずネットワーク上で、複製数の譲渡元となる装置が複数稼働している場合に、いずれの装置に譲渡を要求するかを決定する。

【０３５８】

前記要求装置は、所望のコンテンツを識別するコンテンツ確認情報と、譲渡を希望する複製要求数を含む複製数譲渡要求を、ネットワーク上にブロードキャスト送信する（Ｓ２３０１）。

前記複製要求数は、８桁の数字であり、上から２桁がグループ内装置残数、上から３、４桁目がグループ外装置残数、上から５、６桁目がグループ内媒体残数、上から７、８桁目がグループ外媒体残数であるとする。

【０３５９】

例えば、譲渡を要求するグループ内装置残数が８０、グループ外装置残数が２、グループ内媒体残数が５０、グループ外媒体残数が３である場合、前記複製要求数は、８００２５００３となる。

前記配信装置は、ブロードキャストされた前記コンテンツ確認情報で識別されるコンテンツを管理し、かつ、前記複製要求数に含まれる各残数以上のグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数を保持している場合、譲渡可と判定し、それ以外の場合譲渡不可と判定する（Ｓ２３０２）。

【０３６０】

前記配信装置は、譲渡不可であった場合（Ｓ２３０２：ＮＯ）、処理を終了する。

同様に、前記他装置は、ブロードキャストされた前記コンテンツ確認情報で識別されるコンテンツを管理し、かつ、前記複製要求数に含まれる各残数以上のグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数を保持している場合、譲渡可と判定し、それ以外の場合譲渡不可と判定する（Ｓ２３０３）。

【０３６１】

前記他装置は、譲渡不可であった場合（Ｓ２３０３：ＮＯ）、処理を終了する。

前記配信装置は、譲渡可であった場合（Ｓ２３０２：ＹＥＳ）、譲渡可を示す譲渡可否通知を前記要求装置に送信する（Ｓ２３０４）。

前記他装置は、譲渡可であった場合（Ｓ２３０３：ＹＥＳ）、譲渡可を示す譲渡可否通知を前記要求装置に送信する（Ｓ２３０５）。

【０３６２】

前記要求装置は、受信した各譲渡可否通知の内容を確認し、譲渡可を示す譲渡可否通知

の装置の送信元ＩＰアドレスを保持する（Ｓ２３０６）。
前記要求装置は、前記保持したＩＰアドレスを持つ各装置に対し、ＩＣＭＰエコーメッセージを送信し、前記送信の応答であるＩＣＭＰエコーリプライメッセージを受信するまでの各応答時間を測定する。
【０３６３】
前記要求装置は、前記配信装置に対し、ＩＣＭＰエコーメッセージを送信する（Ｓ２３０７）。
前記配信装置は、ＩＣＭＰエコーメッセージを受信し、応答として前記要求装置に対し、ＩＣＭＰリプライメッセージを送信する（Ｓ２３０８）。
前記要求装置は、ＩＣＭＰエコーリプライメッセージを受信し、応答時間を計算する。
【０３６４】
前記要求装置は、他装置に対し、ＩＣＭＰエコーメッセージを送信する（Ｓ２３０９）。
前記他装置は、ＩＣＭＰエコーメッセージを受信し、応答として要求装置に対し、ＩＣＭＰエコーリプライメッセージを送信する（Ｓ２３１０）。
前記要求装置は、ＩＣＭＰエコーリプライメッセージを受信し、応答時間を計算する。
【０３６５】
前記要求装置は、譲渡元装置として、応答時間の最短であった装置を選択する（Ｓ２３１１）。
前記要求装置は、前記譲渡元装置のＩＰアドレスを保持しておく。
ここで、前記要求装置は、前記譲渡元装置として、前記配信装置を選択したものとする。
【０３６６】
前記要求装置と前記配信装置は、図４３及び図４４に示す相互認証と鍵共有を行う（Ｓ２３１２）。
配信装置と、要求装置とは、Ｓ２３１２の実行結果としてセッション鍵を共有する。
前記セッション鍵の共有が完了以後は、配信装置と要求装置との間の通信は、前記セッション鍵を用いて暗号化復号化される。
【０３６７】
前記要求装置は、前記配信装置に対し、前記グループ所属情報と、前記複製要求数とを送信する（Ｓ２３１３）。
前記配信装置は、受信した前記グループ所属情報と、認証部２１０３で保持しているグループ所属情報とが一致しているか否かを確認し、一致している場合グループ内であり、一致しない場合グループ外と判定する（Ｓ２３１４）。
【０３６８】
前記配信装置は、グループ内と判定した場合（Ｓ２３１４：ＹＥＳ）、複製制限情報管理部２１０２に保持している、グループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数から、前記複製要求数が示す各残数を引く（Ｓ２３１５）。
例えば、前記配信装置が保持するグループ内装置残数が９９、グループ外装置残数が１０、グループ内媒体残数が９９、グループ外媒体残数が１０であり、前記複製要求数が値「３００５１００１」の場合、Ｓ２３１５を実行したのち、前記配信装置は、グループ内装置残数として値「６９」、グループ外装置残数として値「５」、グループ内媒体残数として値「８９」、グループ外媒体残数として値「９」を保持することとなる。
【０３６９】
前記配信装置は、譲渡複製数を、値「３００５１００１」とする。
グループ外であった場合（Ｓ２３１４：ＮＯ）、前記譲渡複製数を値「０」とする。
前記配信装置は、前記譲渡複製数と、保持している前記使用期限情報を含む譲渡許可通知を前記要求装置に送信する（Ｓ２３１６）。
前記要求装置は、受信した前記譲渡複製数が０か否かを判定する（Ｓ２３１７）。
【０３７０】

前記譲渡複製数が０であった場合（Ｓ２３１７：ＹＥＳ）、要求装置は処理を終了する。

前記譲渡複製数が０でなかった場合、要求装置中の複製制限情報管理部２２０２は、前記コンテンツ確認情報をコンテンツ識別子とし、前記コンテンツ識別子と譲渡複製数と前記使用期限情報とを対応づけて、複製制限管理情報として保持する（Ｓ２３１８）。

４．３．５　使用期限管理処理

予め使用期限の定められたコンテンツを、配信装置から、要求装置へ複製した場合の処理について説明する。

【０３７１】

前記配信装置、前記要求装置それぞれが備える時計が前記使用期限を示す時刻に到達した場合、前記要求装置は前記コンテンツの消去を行い、前記配信装置は、前記消去したコンテンツに対応した複製許可の残数を増やす処理を行う。

図４７は、使用期限の定まったコンテンツを管理する使用期限管理処理を示す。

図４７中、配信装置はサーバ２００１であるとし、要求装置は、再生装置２００２であるとする。

【０３７２】

前記配信装置は、前記要求装置との間で、図４５に示したように、コンテンツの複製を行う（Ｓ２４０１）。

前記配信装置は、Ｓ２２１２における、前記要求装置へのコンテンツの送信時に、前記使用期限情報を送信するものとする。

前記要求装置は、受信した前記使用期限情報を保持する。

【０３７３】

前記配信装置は、時間管理部２１０５に対し、時間管理部２１０５中の時計が前記使用期限情報を刻んだ場合に通知するよう指示する（Ｓ２４０２）。

前記要求装置は、時間管理部２２０５に対し、時間管理部２２０５中の時計が前記使用期限情報を刻んだ場合に通知するよう指示する（Ｓ２４０２）。

前記配信装置は、時間管理部２１０５からの前記通知があった場合（Ｓ２４０２：ＹＥＳ）、前記要求装置に対応する残数を、１増加させる（Ｓ２４０３）。

【０３７４】

例えば、前記要求装置が、グループ内の装置である場合には、前記複製制限管理情報中のグループ内装置残数を１増加させ、前記要求装置がグループ外の装置である場合には、前記複製制限管理情報中のグループ外装置残数を１増加させる。

前記要求装置は、時間管理部２２０５からの前記通知があった場合（Ｓ２４０４：ＹＥＳ）、前記使用期限情報に対応する前記コンテンツを消去する（Ｓ２４０５）。

４．３．６　複製予約実行処理

図４８は、コンテンツの複製予約実行処理を示す図である。

【０３７５】

配信装置、要求装置、他装置は、それぞれ、図４２に示すコンテンツ複製元決定処理を行う（Ｓ２５０１）。

ここで、前記配信装置はホームサーバ２００１、前記要求装置は、再生装置２００２、前記他装置は、再生装置２００３であるとする。

前記要求装置は、Ｓ２５０１により、複製元として、前記配信装置を選択したものとする。

【０３７６】

前記配信装置は、Ｓ２５０１中で取得した、複製を希望するコンテンツを識別するコンテンツ確認情報を保持しておく。

前記要求装置は、前記配信装置に対し、前記複製を実際に開始する複製開始時刻を含む複製予約要求を送信する（Ｓ２５０２）。

前記配信装置は、前記複製予約要求を受信し、時間管理部２１０５に、前記複製開始時刻になった場合を検出するようタイマー設定する（Ｓ２５０３）。

【０３７７】
前記配信装置は、時間管理部２１０５において、前記複製開始時刻になったことを検出する（Ｓ２５０４）。
前記要求装置と、前記配信装置とは、図４５のＳ２２０３以降の処理を実行し、コンテンツの複製を行う（Ｓ２５０５）。
４．３．７　コンテンツ返却処理
配信装置から要求装置へコンテンツの複製を行った後、前記要求装置側で前記コンテンツの消去を実行し、前記配信装置側で、前記要求装置側での前記消去に対応する残数を１増加させ前記コンテンツを複製出来る残数を１増やすことをコンテンツ返却処理と称す。
【０３７８】
図４９は、コンテンツ返却処理を示すフローチャートである。
ここで、前記要求装置は再生装置２００２であり、前記配信装置はホームサーバ２００１であるとする。
また、前記配信装置は、前記要求装置に対して、コンテンツを複製しているものとする。
【０３７９】
前記要求装置は、前記配信装置に対し、返却するコンテンツを識別するコンテンツ確認情報を含む、コンテンツ返却要求を送信する（Ｓ２６０１）。
前記配信装置は、受信したコンテンツ返却要求を保持する。
前記要求装置と、前記配信装置とは、図４３及び図４４に示した相互認証と鍵共有処理を実行する（Ｓ２６０２）。
【０３８０】
前記要求装置は、Ｓ２６０２を実行することにより、前記配信装置とセッション鍵を共有する。
前期要求装置は、前期配信装置に対し、前記グループ所属情報を送信する（Ｓ２６０３）。
前記配信装置は、前記受信したグループ所属情報と、自身が保持しているグループ所属情報とが一致するか否かを調べ、一致する場合、前記要求装置がグループ内であると判定し、一致しない場合は、前記要求装置がグループ外であると判定する（Ｓ２６０４）。
【０３８１】
前記要求装置がグループ外であった場合（Ｓ２６０４：ＮＯ）、前記配信装置は、前記要求装置にエラー通知を送信し（Ｓ２６０５）、処理を終了する。
前記要求装置は、前記エラー通知を受信した場合（Ｓ２６０６：ＹＥＳ）、処理を終了する。
前記要求装置がグループ内であると判定した場合（Ｓ２６０４：ＹＥＳ）、前記要求装置は、前記コンテンツ返却要求を形式変換して前記要求管理情報として要求管理キューにキューイングする（Ｓ２６０７）。
【０３８２】
前記配信装置は、前記コンテンツ返却要求に係る前記要求管理情報が、要求管理キューの先頭になるのを検出する（Ｓ２６０８）。
前記コンテンツ返却要求が要求管理キューの先頭になった場合（Ｓ２６０８：ＹＥＳ）、前記配信装置は、前記コンテンツ確認情報を含む返却処理開始通知を、要求装置に対し送信する（Ｓ２６０９）。
【０３８３】
前記返却処理開始通知を受信した要求装置は、前記返却処理開始通知に含まれるコンテンツ確認情報が識別するコンテンツを消去する（Ｓ２６１０）。
前記要求装置は、前記配信装置に対し、前記コンテンツ確認情報を含むコンテンツ消去完了通知を送信する（Ｓ２６１１）。
前記配信装置は、前記消去に対応する前記対象残数を１増加させる（Ｓ２６１２）。
【０３８４】

前記配信装置は、前記要求管理キュー先頭から、前記コンテンツ返却要求を削除し、前記要求管理キューを更新する（Ｓ２６１３）。

４．４　変形例

（１）　媒体は、装置を介して、ホームサーバに接続しているが、ホームサーバに媒体挿入口を設け、挿入口に挿入された媒体と、ホームサーバとを接続し、相互に認証、コンテンツのコピー等を行ってもよい。

【０３８５】

媒体と、ホームサーバとの間に再生装置とネットワークとを介するのと、直接接続するのとの違いであり、相互の認証、コンテンツの複製等の方法に違いは生じない。

（２）コンテンツ配布元決定部２２０６は、コンテンツの配布元を決定するために、ＩＣＭＰエコーメッセージとＩＣＭＰエコーリプライメッセージとを用いなくてもよい。

コンテンツ配布元決定部２２０６は、各装置の情報処理能力を予め記憶しておき、プロードキャストに対し応答してきた装置の中で、情報処理能力の一番高い装置をコンテンツの配布元と決定してもよい。

【０３８６】

また、コンテンツ配布元決定部２２０６は、各装置の優先度を予め設定し、プロードキャストに対し応答してきた装置の中で、最も優先度の高い装置を前記コンテンツの配布元としてもよい。

（３）複製管理情報は、使用期限情報を含んでいるが、その他の情報を用いて、コンテンツの複製制限を加えてもよい。

【０３８７】

例えば、複製制限情報管理部は、地域制限情報を保持していてもよい。

前記地域制限情報は、前記コンテンツを複製してもよい地域を示す情報である。

前記地域制限情報は、値として、例えば、日本を示す値「１」、米国を示す値「２」、ドイツを示す値「３」を取りうるものとする。

前記地域制限情報の値が「１」であった場合は、コンテンツの複製を、日本国内にある装置に対してのみに制限する。

【０３８８】

また、複製制限情報管理部は、リボケーションリストを保持していてもよい。

前記リボケーションリストは、前記コンテンツの複製の許可が与えられない装置を示すリストである。

前記リボケーションリストが示す装置に対しては、複製制限情報管理部２１０２は、前記コンテンツの複製許可を与えない。

【０３８９】

また、複製制限情報管理部は、複製世代情報を保持していてもよい。

前記複製世代情報は、コンテンツの再度の複製を何回許すかを示す。

例えば、前記複製世代情報が２であるコンテンツは、いわゆる、子コピーと孫コピーまでが許可されることとなる。

（４）コンテンツ複製管理システムは、課金システムと協働してもよい。

【０３９０】

本システムが、グループ外装置に対し、コンテンツの複製許可を与えると判断した場合に、課金システムに対し、課金依頼を送信する。

前記課金依頼には、コンテンツの利用者と、課金金額が含まれる。

前記課金システムは、予め、コンテンツの利用者と契約を行い、課金が発生した場合の、例えばクレジットカードを用いて精算する等の契約を行っている。

【０３９１】

精算処理が滞りなく実施された場合に、前記課金システムは、サーバに対し、精算処理の終了を通知する。

精算処理の終了通知を受け、前記サーバは、要求装置に対し、コンテンツの複製許可を与えた後、コンテンツの複製を行う。

あるいは、家庭内ネットワークの中であっても、コンテンツの複製が行われるたびに、課金してもよい。

【０３９２】

（５）実施形態中で、再生装置２００２が、ホームサーバ２００１から、コンテンツの複製を許可する権利の譲渡を受ける形態について説明したが、再生装置２００２は、ホームサーバ２００１が稼動できなくなった場合にバックアップ機として稼動することとしてもよい。

（６）複製管理情報として、装置に関して前記グループ内装置残数と、前記グループ装置残数とを管理し、記憶媒体に対して前記グループ内媒体残数と、前記グループ外媒体残数とを管理しているが、管理上、前記装置と前記記憶媒体とを区別せず、前記グループ内装置残数と前記グループ内媒体残数との合計数をグループ内許可残数として管理し、前記グループ外装置残数と前記グループ外媒体残数との合計数をグループ外許可残数として管理してもよい。

【０３９３】

（７）ホームサーバは、ネットワークを通じて複製制限情報を放送とは別に取得することとしているが、取得経路はネットワークに限るものではない。

放送局が放送により複製制限情報を送信し、ホームサーバが当該放送を受信することにより前記複製制限情報を取得することとしてもよい。

（８）コンテンツ複製元決定処理において、要求装置は、コンテンツ確認要求をネットワーク上にブロードキャスト送信しているが、ブロードキャスト以外を用いてもよい。

【０３９４】

例えば、所望のコンテンツの配布元となりうる装置の候補が予め定められている場合には、要求装置は、コンテンツ確認要求を、マルチキャスト送信してもよい。

（９）　複製制限情報管理部は、要求管理キューに繋がれた要求管理情報について、前記要求管理キューの先頭に繋がれた要求管理情報に対する処理を行っているが、キューの先頭に繋がれた要求管理情報に係る残数（グループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数のうちのいずれか）が０であり処理区分で示される処理が出来ない場合に、キューの先頭以外に繋がれた要求管理情報であって、処理区分が消去を示す要求管理情報を先に処理してもよい。

【０３９５】

複製制限情報管理部は、処理区分が消去である要求管理情報を優先して処理することにより前記残数が１増加するため、キューの先頭に繋がれた要求管理情報に関する処理を行うことが出来る。

５．　その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）本実施の形態で、ＡＤ内サーバ１００と接続されていない機器を登録する際に、ＩＣカード４００を用いてＣＳＩをコピーするとしたが、クライアント機器間でＣＳＩを移動するとしても良い。

【０３９６】

再生装置２００から再生装置２００ｎにＣＳＩを移動し、再生装置２００ｎをＡＤ内機器として登録する際を例として説明する。

再生装置２００と再生装置２００ｎとを接続し、再生装置２００ｎを操作して移動通知を再生装置２００に送信する。再生装置２００及び再生装置２００ｎは、ＳＡＣを確立してセッション鍵ＳＫを生成する。再生装置２００は、セッション鍵ＳＫでＣＳＩを暗号化して再生装置２００ｎへ送信する。再生装置２００ｎは、セッション鍵を用いて暗号化ＣＳＩを復号して格納し、ＳＡＣ確立の際に受け取った移動元である再生装置２００のＩＤを記憶する。また、再生装置２００へ受領通知を送信する。再生装置２００は、受領通知を受信すると、ＣＳＩ格納部２０８のＣＳＩを削除して、「０」を格納する。

【０３９７】

再生装置２００ｎは、ＡＤ内サーバ１００に接続され、ＳＡＣを確立すると、ＡＤ内サーバ１００にＣＳＩを移動されたことを通知し、移動元のＩＤ及び再生装置２００ｎのＩＤを送信し、ＡＤ内サーバ１００は、登録情報の機器ＩＤを書き換える。

（２）ＩＣカード４００はＡＤ内サーバ１００に付属の機器であるとしたが、付属でなくても良い。

【０３９８】

ＩＣカード４００も他のクライアント機器と同様に、ＡＤ内サーバ１００に接続されるとＳＡＣを確立し、ＩＤ＿４を機器ＩＤとして登録し、ＣＳＩを取得する。

ＡＤ内サーバ１００は、ＤＶＤ５００にコンテンツ鍵を記録する際、コンテンツ鍵をＩＣカード４００のＩＤ＿４とＣＳＩとを連結して生成した暗号鍵を用いて暗号化する。

車載機器３００は、ＤＶＤ５００が装着され、ＩＣカード４００が接続されると、ＩＣカード４００との間でＳＡＣを確立してセッション鍵を共有する。

【０３９９】

ＩＣカード４００は、ＩＣカード４００内に記憶しているＩＤ＿４とＣＳＩとを連結して復号鍵を生成し、セッション鍵ＳＫを用いて復号鍵を暗号化して暗号化復号鍵を生成して車載機器３００へ送信する。

車載機器３００は、暗号化復号鍵をセッション鍵ＳＫを用いて復号して復号鍵を生成し、ＤＶＤから読み出す暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、コンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを再生する。

【０４００】

また、上記（１）のように、クライアント間でＣＳＩを移動する場合と同様の処理を行い、ＩＣカードから車載機器３００にＣＳＩを移動しても良い。この場合、実施の形態１のＩＣカード４００と同様に、付属でないＩＣカードに、ＡＤ内サーバ１００へ移動を通知する機能を持たせても良い。車載機器３００にＣＳＩを移動したＩＣカードは、その場でＣＳＩを削除せずに、ＣＳＩの移動を禁止し、ＡＤ内サーバ１００に移動を通知した後にＣＳＩを削除する。

（３）ＩＣカード４００を用いてＡＤ内サーバ１００に接続されていない機器を登録する場合、ネットワークを介してＡＤ内サーバ１００からＩＣカード４００に許可権利又はＣＳＩを送信するとしても良い。

【０４０１】

一例として、ＰＣなどネットワークに接続して通信する機能を有するクライアント機器に、ＩＣカード４００が接続されると、ＩＣカード４００は、ＰＣの通信機能を利用して、ＳＡＣ確立の処理を行い、許可権利又はＣＳＩを受信する。

通信機能を有するクライアント機器は、ＰＣに限らず、ＰＤＡや携帯電話などであっても良い。

（４）本実施の形態では、ＡＤ内サーバ１００からクライアント機器へコンテンツを配送、又はＤＶＤに記録して配布するとしたが、クライアント機器間でＳＡＣを確立してセッション鍵ＳＫを生成し、コンテンツを配送するとしても良い。

（５）本実施の形態で、ＩＣカード４００を用いて車載機器３００を登録するとしたが、同様にＩＣカード４００を用いて、脱退の処理を行っても良い。

【０４０２】

この場合、ＩＣカード４００を接続された車載機器３００を操作して、ＩＣカード４００へ脱退要求を送信し、ＩＣカード４００は、ＳＡＣを確立して車載機器３００が登録済みであることを確認し、車載機器３００へ削除通知を送信する。車載機器３００は、ＣＳＩを削除し、ＩＣカード４００へ削除完了通知を送信する。ＩＣカード４００は、削除完了通知を受信すると、脱退した車載機器３００のＩＤを記憶する。ＩＣカード４００は、ＡＤ内サーバ１００に接続されると、ＡＤ内サーバ１００に、車載機器３００が脱退した旨と、車載機器３００のＩＤとを通知する。ＡＤ内サーバ１００は、機器ＩＤから車載機器３００のＩＤを削除し、登録台数から「１」減算し、残数に「１」を加算する。

（６）本実施の形態でＡＤ内サーバ１００は、ＳＡＣを確立する際の署名検証で相手機器

が格納しているＣＳＩの値によって、相手機器が未登録であるか登録済みであるかを確認するとしたが、認証する機器からＩＤを受信し、登録情報の機器ＩＤに、受信したＩＤが記憶されているか否かによって、未登録か、登録済みかを確認するとしても良い。また、ＡＤ内の機器として登録されているクライアント機器全てが、登録されているＩＤを記憶しておき、クライアント機器間でも同様に、ＩＤによって、登録、未登録を確認するとしても良い。

（７）ＡＤ内サーバ１００と接続されていない機器を登録する際、ＩＣカード４００を用いるとしたが、ＡＤ内サーバ１００がＣＳＩを表示部１１４に表示し、それをユーザがクライアント機器に手入力するとしても良い。この場合、入力するコードは、機器やセッションに依存してＣＳＩを暗号化した値であっても良い。

（８）本実施の形態で、ＳＡＣを確立し、ＣＳＩを暗号化して送信する際、暗号文に暗号化ＣＳＩを送信する機器の署名データを付加して送信するとしても良い。

（９）本実施の形態で、登録情報及びＣＳＩは、それぞれの機器の内部に格納されるとしたが、着脱可能で、許可なく読み出し、書き込み及びコピーが出来ない領域に格納するとしても良い。

（１０）本実施の形態で、コンテンツを暗号化する際の暗号化鍵、又は復号する際の復号鍵として、機器のＩＤ及びＣＳＩ又は乱数及びＣＳＩを連結して利用するとしたが、この限りではなく、機器のＩＤ及びＣＳＩ又は乱数及びＣＳＩを用いて演算を行い、その結果得られる値を用いるとしても良い。

（１１）本実施の形態では、登録情報として、最大数、登録台数及び残数を管理するとしたが、これに限らない。

【０４０３】

最大数を残数の初期値とし、登録する度に残数から「１」ずつ減らし、残数が「０」でなければクライアント機器を登録するとしてもよい。また、最大数と、登録台数とを管理し、登録台数が最大数以下であれば、クライアント機器を登録するとしても良い。

（１２）登録情報の機器の台数は、ＡＤ内サーバ１００とオンラインで接続している機器と、ＩＣカード４００を用いて登録する機器とを分けて、最大数、登録台数などを管理しても良い。

（１３）本実施の形態では、ＡＤ内サーバ１００が記憶している登録情報を基に管理しているが、別途管理機関を設け、以下（ａ）～（ｃ）のようにしても良い。

【０４０４】

（ａ）管理機関が最大数を設定し、最大数に管理機関の署名データを付して、ＤＶＤなどの可搬型の記録媒体に記録して配布、又は通信を介して配布する。ＡＤ内サーバ１００は、署名データを検証し、検証結果が成功の場合に、最大数として記憶する。

（ｂ）ＡＤ内サーバ１００は、登録したい台数を管理機関に要求する。管理機関は、台数に応じた課金を行い、課金に成功した場合に、要求した台数の登録を許可する情報をＡＤ内サーバ１００へ送信し、ＡＤ内サーバ１００は情報を受け取ると、許可された台数の範囲内でクライアント機器の登録を受け付ける。

【０４０５】

（ｃ）ＡＤ内サーバ１００は、クライアント機器からの登録を受け付ける度に、管理機関に要求を出し、管理機関は、要求に対して課金を行い、課金に成功すると、登録を許可する。ＡＤ内サーバ１００は、許可されると、クライアント機器を登録し、ＣＳＩを送信する。

（１４）再生装置２００は、ＡＤ内サーバ１００から配送されたコンテンツを再生するとしたが、ＤＶＤ再生機能を有し、ＡＤ内サーバ１００によってＤＶＤ５００に記録されたコンテンツを再生するとしても良い。

【０４０６】

また、ＡＤ内サーバ１００は、登録情報に記憶している機器ＩＤ全てを、それぞれＣＳＩと連結してコンテンツ鍵の暗号化に用いるとしたが、ＤＶＤを再生する機能を有する機器のＩＤを予め記憶しておき、ＤＶＤを再生できる機器のＩＤを抽出し、それぞれＣＳＩ

と連結してコンテンツ鍵の暗号化に用いるとしても良い。
（１５）本実施の形態では、ＡＤ内サーバ１００はＤＶＤにコンテンツを記録するとしたが、メモリーカード、ＭＤ、ＭＯ、ＣＤ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｋ）などに記録するとしても良いし、ＩＣカードにコンテンツを記録するとしても良い。
【０４０７】
また、クライアント機器は、再生装置の他、記録装置でもよく、それらを組み合わせたものであってもよい。また、クライアント機器は、ユーザ宅内に設置されている又は車両に搭載されている他、ユーザが持ち運ぶことができる携帯型の機器であっても良い。
（１６）ＩＣカード４００は、ＡＤ内サーバ１００又は車載機器３００に直接接続されるため、ＳＡＣの確立処理を行わなくても良い。
（１７）ＳＡＣ確立の際、乱数Ｃｈａ＿Ｂ又はＣｈａ＿Ａに、ＣＳＩを連結したデータに対して署名データ生成するとしたが、署名対象と成るデータのハッシュ値を計算し、このハッシュ値に対して署名データを生成するとしても良い。
（１８）ＳＡＣ確立の際、認証相手の機器が未登録か登録済みかを判断するとき及び鍵共有のときにＣＳＩ利用するとしたが、どちらか一方に利用するとしても良い。
【０４０８】
また、本実施の形態では双方向に認証を行っているが、片方向認証であっても良い。
（１９）クライアント機器の登録を、時間で制限するとしても良い。
ＡＤ内サーバ１００とクライアント機器との間で時間を合わせる。ＡＤ内サーバ１００は、ＣＳＩの使用を許可する期間を設定して有効期限情報とし、有効期限情報とＣＳＩとをクライアント機器に送信し、登録台数から「１」減算する。
【０４０９】
クライアント機器は、有効期限情報及びＣＳＩを受信し、格納する。有効期限情報が示す期間が終了すると、ＣＳＩを削除する。
ＡＤ内サーバ１００は、有効期限情報が示す期間が終了すると、登録台数に「１」を加算する。機器ＩＤを記憶している場合は、期限が切れた機器のＩＤを削除する。
なお、有効期限情報は、有効期限の開始と終了の日時を示す情報でも良いし、終了の日時のみ示すものであっても良い。また、ＣＳＩの使用開始からの期間を制限するものであっても良いし、ＣＳＩを使用してクライアント機器が動作している期間を制限するとしても良い。
（２０）本実施の形態では、ＡＤ内サーバは１つであるとして説明したが、一つのＡＤに複数のＡＤ内サーバがあっても良い。
【０４１０】
この場合、クライアント機器は、何れのＡＤ内サーバと通信するかを選択することが出来る。選択方法として、ユーザが設定するとしても良いし、クライアント機器がＡＤ内で、当該クライアントと距離が最短のＡＤ内サーバを選択しても良い。また、ＡＤ内サーバのうち、処理能力が高いものや、他のタスクが少ないＡＤ内サーバを選択するとしても良い。
【０４１１】
また、以下のように、クライアント機器から登録を要求されたＡＤ内サーバが、それ以上クライアント機器を登録出来ない場合、登録可能な他のＡＤ内サーバを探すとしても良い。
クライアント機器は、１つのＡＤ内サーバに登録要求を送信する。登録要求を受信したＡＤ内サーバは、登録台数が最大数と一致する場合、他のＡＤ内サーバに、クライアント機器を登録できるか問い合わせる。他のＡＤ内サーバは、登録可能である場合、要求元のクライアント機器を登録し、ＡＤ内サーバに登録可能である旨を応答し、ＡＤ内サーバは、クライアント機器へＣＳＩを送信する。
【０４１２】
また、他のＡＤ内サーバが登録できない旨を応答した場合、ＡＤ内サーバは、更に他のＡＤ内サーバへ問い合わせる。

また、複数のＡＤ内サーバ間で代表となるＡＤ内サーバを決定し、代表サーバが全てのグループ内機器を管理するとしても良い。この場合、代表で無いＡＤ内サーバがクライアント機器から登録要求を受け付けると、代表サーバに登録可能であるか問い合わせ、登録可能で有る場合、クライアント機器は代表サーバに登録され、代表サーバから要求を受け付けたＡＤ内サーバを介してＣＳＩを受け取る。

【０４１３】

なお、要求を受け付けたＡＤ内サーバが、他の処理を行っている場合などに、他のＡＤ内サーバへ問い合わせるとしても良い。

また、以下（ａ）、（ｂ）のように、複数のＡＤ内サーバ間で、登録した機器の台数を管理するために、登録した機器に関するリストを共有するとしても良い。

（ａ）同一ＡＤ内のＡＤ内サーバＲ及びＡＤ内サーバＳはそれぞれ、クライアント機器を登録すると、登録した機器のＩＤを機器リストとして記憶する。また、ＩＤを書き込むことでリストが更新される度に、バージョン番号を機器リストに対応付けて記憶する。

【０４１４】

ＡＤ内サーバＲ及びＳは、定期的又は不定期に前記機器リストを交換する。ＡＤ内サーバＲは、自分が記憶している機器リストのバージョン番号と、ＡＤ内サーバＳから受け取った機器リストのバージョン番号とを比較し、より新しい方を機器リストとして記憶する。ＡＤ内サーバＳも同様に処理する。これにより、常に最新の機器リストを共有することが出来る。

【０４１５】

なお、一方のＡＤ内サーバの機器リストが更新されるたびに機器リストを交換するとしても良い。また、機器リストだけでなく、登録台数、最大数など、登録情報も、上記と同様に共有するとしても良い。

（ｂ）同一ＡＤ内のＡＤ内サーバＴ及びＡＤ内サーバＵはそれぞれ機器リストＴ及び機器リストＵを保持しており、それぞれクライアント機器を登録する際、機器ＩＤと登録した時刻とを対応付けて格納する。ＡＤ内サーバＴ及びＡＤ内サーバＵは、定期的又は不定期に機器リストを交換する。

【０４１６】

ＡＤ内サーバＴは、自分が登録情報として記憶している登録台数が最大数より少なければ、ＡＤ内サーバＵから受け取った機器リストＵに、新しく登録されたクライアント機器を、登録された順に、自分が保持している機器リストＴに書き込む。また、ＡＤ内サーバＵも同様に、機器リストＴを受け取り、新しく登録された順に機器リストＵを更新する。

なお、予めクライアント機器に優先順位を付しておき、優先順位が高い機器を優先的に登録するとしても良い。また、ＡＤ内サーバＴ及びＵに新しく登録されたクライアント機器を合わせると最大数を超える場合、優先順位の高い機器を優先的に登録するとしても良いし、ユーザが登録する機器を選択しても良い。

【０４１７】

この方法によると、一方のＡＤ内サーバが電源を切っていても、他方のＡＤ内サーバに登録でき、他方のＡＤ内サーバが更新されると、機器リストを交換して整合性を保つので、ＡＤ内サーバ間で同一の機器リストを共有することが出来る。

（２１）各ＡＤのＣＳＩの重複を回避するために、それぞれのＡＤを管理するＡＤ内サーバ間で情報を交換して、重複しているか否かを確認するとしても良い。

【０４１８】

また、安全性を高めるために、ＡＤ内サーバは、それぞれのＣＳＩをハッシュ関数に入力してハッシュ値を算出し、ハッシュ値を交換して重複しているか確認するとしても良い。

また、ＡＤ内サーバがＣＳＩを生成する代わりに、管理機関を設けて、管理機関が全てのＡＤのＣＳＩを重複しないように生成し、各ＡＤ内サーバに安全に送付するとしても良い。

（２２）クライアント機器は複数のＡＤに属するようにしてもよい。

【０４１９】
また、クライアント機器が、格納できるＣＳＩの数を制限することで、登録出来るＡＤの数を制限するとしても良い。また、各ＡＤ内サーバが登録されているクライアント機器のリスト情報を交換して、１つのクライアント機器が登録できるＡＤの個数を制限する構成であっても良い。また、リスト情報の交換により、クライアント機器がいくつのＡＤに属しているかを確認することが出来る。
【０４２０】
別途、クライアント機器が登録しているＡＤの数を管理する管理機関を設けても良い。
また、１台のＡＤ内サーバは、複数のＡＤを管理するとしても良い。この場合、ＡＤ内サーバは、それぞれ異なるＣＳＩを格納できる数を制限されており、この数以内のＡＤを管理できる。また、ＡＤ内サーバは、登録可能なクライアント機器の台数をＣＳＩ毎に記憶していても良いし、ＣＳＩとグループのＩＤとを対応付けて記憶するとしても良い。
（２３）ＡＤは、それぞれ識別子を割り当てられており、コンテンツを配送する際に、コンテンツの配送元の機器は、当該機器が登録しているＡＤの識別子を電子透かしとしてコンテンツに埋め込むとしても良い。
【０４２１】
これにより、クライアント機器が復号したコンテンツを、不正にＡＤ外に配布した場合に、そのコンテンツがどのＡＤから流出したのかを特定することが出来る。更に、コンテンツの配信元のサーバが、各ＡＤに登録しているクライアント機器のＩＤを管理している場合、コンテンツを流出したクライアント機器のＩＤをＣＲＬに載せても良い。
（２４）本実施の形態では、機器の認証後にコンテンツを配送するとしたが、本発明はこれに限定されない。
【０４２２】
コンテンツを配送する際、以下のように、認証を行わないとしても良い。
コンテンツの送信側の機器は、ＣＳＩを基にして暗号鍵を生成する。生成した暗号鍵を用いてコンテンツ鍵を暗号化し、暗号化コンテンツと暗号化コンテンツ鍵とを配送する。
受信側の機器は、暗号化コンテンツと暗号化コンテンツ鍵とを取得すると、ＣＳＩを基にして、暗号鍵と同一の復号鍵を生成する。生成した復号鍵を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、コンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを生成する。
【０４２３】
これによると、ＣＳＩを保持する機器のみが復号鍵を生成し、コンテンツを復号することが出来る。
また、認証せずに、暗号化コンテンツのみ配送し、その後、実施の形態と同様に認証を行ってセッション鍵を共有し、認証に成功した場合に、セッション鍵でコンテンツ鍵を暗号化して配送するとしても良い。
【０４２４】
なお、暗号化コンテンツの配送は、通信で配送するとしても良いし、可搬型の記録媒体に記録して配布するとしても良い。
また、受信側の機器からの要求に応じてコンテンツを配送する他、要求がなくても送信側の機器が判断して配送するとしても良いし、外部からの入力に従って、配送するとしても良い。
（２５）本実施の形態で、ＣＳＩ格納部は、初期値として「０」を記憶しており、ＡＤ内サーバ１００が生成したＣＳＩを取得すると、取得したＣＳＩを上書きするとしたが、初期値とＣＳＩとを別の領域に記憶しても良い。また、取得したＣＳＩを初期値とは別の領域に記憶すると、初期値の使用を抑制するとしても良い。
【０４２５】
なお、使用を抑制した初期値は、移動、脱退などでＣＳＩを削除した際に、再度活性化される。
なお、未登録を示す値として「０」を格納するとしたが、「０」でなくても良く、ＣＳ

Ｉとして生成される値と異なる値であればよい。
（２６）本実施の形態でＡＤ内サーバ１００はＩＣカード４００にＣＳＩのコピーを１回許可しているが、複数回の許可を与えても良い。
【０４２６】
また、ＩＣカード４００は、ＣＳＩを用いてクライアント機器を認証する他、ＣＳＩをコピーしたクライアント機器のＩＤを記憶しておき、コピーする際にクライアント機器のＩＤを確認することで、同じクライアント機器へ複数回ＣＳＩをコピーすること防ぐとしても良い。
また、クライアント機器の登録処理を行う機能をＩＣカードに実装し、ＩＣカードを接続された機器がＡＤ内サーバとして動作するとしても良い。
【０４２７】
また、クライアント機器が複数のクライアント機器の代表としてＡＤ内サーバに登録し、他の複数のクライアント機器にＣＳＩをコピーする権利を受けるとしても良い。以下に、図５０を用いて一例を示す。
ユーザ宅にはＡＤ内サーバ６００と、クライアント機器６０１とが設置されており、クライアント機器６０１は既にＡＤ内サーバ６００に登録されている。ＡＤ内サーバ６００は、登録情報として最大と残数とを記憶しており、ここでは最大が４、残数が３であるとする。
【０４２８】
ユーザが所有する車両には、ＡＤ内サーバ６００に登録されていない車載機器６０２．６０３．６０４が搭載されている。車載機器６０３．６０４は、ＡＤ内サーバ６００と直接通信する機能を持たない。車載機器６０２は、可搬型でＡＤ内サーバ６００と直接通信する機能を有する。また、車載機器６０２～６０４は、それぞれ接続して通信可能である。
【０４２９】
車載機器６０２は、車載機器の代表として、ＡＤ内サーバ６００に接続されると、登録したいクライアント機器の台数である希望台数３を含む登録要求をＡＤ内サーバ６００へ送信する。
ＡＤ内サーバ６００は、登録要求を受信すると、実施の形態と同様に車載機器６０２を認証し、セッション鍵を共有する。認証に成功した場合、登録要求に含む希望台数が、登録情報として記憶している残数以下であるかを判断する。残数以下であると判断する場合、記憶しているＣＳＩを読み出し、読み出したＣＳＩと、３台分の登録を許可する許可権利とを、セッション鍵を用いて暗号化し、暗号化権利情報として車載機器６０２に送信する。
【０４３０】
車載機器６０２は、暗号化権利情報を受信すると、セッション鍵を用いて復号し、ＣＳＩ及び許可権利を生成する。また、生成したＣＳＩを記憶することで、許可権利の内、１台分の許可権利を使ったので、残り２台登録できることを示す許可権利を記憶する。また、車載機器６０３及び６０４と、それぞれ認証を行い、成功するとＣＳＩを送信し、送信した台数分の許可権利を減らす。
【０４３１】
これによって、車載機器６０２～６０４をクライアント機器として登録できる。
なお、残数が希望台数未満である場合、残数が示す台数分だけ登録を許可する許可権利を送信する。例として、２台分の許可権利を送信した場合、車載機器６０２は、ＣＳＩを記憶することで１台分の許可権利を使い、車載機器６０３．６０４の何れかにＣＳＩを送信することでもう１台分の許可権利を使う。ＣＳＩの送信先の機器は、ユーザが選択するとしても良いし、それぞれの機器が予め優先順位を有し、優先順位の高い機器に送信するとしても良い。
【０４３２】
また、車載機器６０２～６０４をＡＤ内サーバ６００に登録する際、各車載機器のＩＤ

をＡＤ内サーバ６００に登録する場合、以下のように処理する。
車載機器６０２は、登録する前に、車載機器６０３及び６０４のＩＤを取得する。ＡＤ内サーバ６００に登録する際、取得したＩＤと、車載機器６０２自身のＩＤとをＡＤ内サーバ６００に送信する。ＡＤ内サーバ６００は、受信したＩＤを機器ＩＤとして記憶する。また、残数が希望台数未満である場合、ＡＤ内サーバ６００は、受け取ったＩＤの内、残数が示す台数分のＩＤを記憶する。この場合、登録するＩＤをユーザが選択するとしても良いし、予めＩＤに優先順位を付し、優先順位の高いＩＤから順に残数が示す台数分のＩＤを記憶するとしても良い。
【０４３３】
また、車載機器６０２は、許可権利が余ると、ＡＤ内サーバ６００に返すことが出来る。
なお、車載機器６０２は、当該車載機器６０２の権利を含めた許可権利を取得するとしたが、車載機器６０２は、実施の形態と同様にＡＤ内サーバ６００に登録し、車載機器６０３及び６０４にＣＳＩをコピーする権利を取得するとしても良い。
（２７）複数のＡＤを合わせて１つのＡＤを形成しても良い。
【０４３４】
一例として、ＡＤ＿ＥとＡＤ＿Ｆとを合わせて、ＡＤ＿Ｇを形成する場合を図５１、を用いて説明する。
ＡＤ＿Ｅ及びＡＤ＿Ｆは、それぞれ１台のＡＤ内サーバと、図示していない複数のクライアント機器とから構成される。ＡＤ＿ＥのＡＤ内サーバＥは、最大ｍ台のクライアント機器が登録可能であり、ＡＤ＿Ｅ内の機器は、それぞれＣＳＩ＿Ｅを保持している。また、ＡＤ＿ＦのＡＤ内サーバＦは、最大ｎ台のクライアント機器が登録可能であり、ＡＤ＿Ｆ内の機器は、それぞれＣＳＩ＿Ｆを保持している。
【０４３５】
この２つのＡＤからＡＤ＿Ｇを形成する。まず、ＡＤ内サーバＥとＡＤ内サーバＦとの間で、ＡＤ＿Ｇを管理するＡＤ内サーバＧとなる機器を決定する。この際、処理性能、各ＡＤ内サーバの優先順位などを基に決定しても良いし、ユーザが決定しても良い。ＡＤ内サーバＧでない方のＡＤ内サーバは、クライアント機器としてＡＤ＿Ｇに登録される。
ＡＤ内サーバＧに登録可能な台数ｋは、ｍ、ｎ又はｍとｎとの平均とする。また、ＡＤ内サーバＧは、新たにＣＳＩ＿Ｇを生成して、各クライアント機器を認証し、認証に成功した機器へＣＳＩ＿Ｇを送信する。
【０４３６】
ＡＤ＿ＥとＡＤ＿Ｆとを形成する機器の合計が、台数ｋを超える場合、登録する機器が選択される。この場合、予め設定されている優先順位を下にＡＤ内サーバＧが選択しても良いし、ユーザが選択するとしても良い。
なお、上述のように、２つのＡＤから新たに１つのＡＤを形成するほか、一方のＡＤに他方のＡＤを足しても良い。ＡＤ＿ＥにＡＤ＿Ｆを足す場合、ＡＤ＿Ｆ内の機器はＡＤ＿Ｅのクライアント機器としてＡＤ内サーバＥに登録され、ＣＳＩ＿Ｅを保持する。この際、登録するクライアント機器の台数が最大ｍ台を超える場合、上述のように、登録する機器が選択される。
【０４３７】
なお、ｍ、ｎ及びｋは、正の整数である。
（２８）１つのＡＤから複数のＡＤに分割するとしても良い。
一例として、ＡＤ＿ＨからＡＤ＿ＩとＡＤ＿Ｊを形成する場合を、図５２を用いて説明する。
ＡＤ＿Ｈは、ＡＤ＿Ｈ内の機器を管理するＡＤ内サーバＨと、図示していない複数のクライアント機器とから構成される。
【０４３８】
ＡＤ内サーバＨは、Ｐ台（Ｐは正の整数）のクライアント機器が登録可能であり、ＡＤ＿Ｈ内の各機器はＣＳＩ＿Ｈを格納している。

ＡＤ内サーバＨは、ＡＤ＿Ｉ及びＡＤ＿Ｊを形成する際、ＡＤ＿Ｈ内のクライアント機器から新たにＡＤ内サーバＩ及びＡＤ内サーバＪとなる機器を選択する。この際、処理能力が高い機器をＡＤ内サーバとしても良いし、予め各機器に付されている優先順位を基に選択しても良い。また、ユーザが選択しても良いし、クライアント機器間で処理能力、優先順位などを基に選択しても良い。なお、ＡＤ内サーバＨがＡＤ内サーバＩ又はＡＤ内サーバＪとして、新たなＡＤを形成するとしても良い。

【０４３９】

分割後、それぞれに属するクライアント機器が選択される。この際、優先順位を基にそれぞれのＡＤ内サーバが選択しても良いし、ユーザが選択しても良い。ＡＤ内サーバＩ及びＪは、それぞれ最大Ｐ台のクライアント機器を登録可能である。また、各ＡＤのクライアント機器を選択すると、ＡＤ内サーバＩは、ＣＳＩ＿Ｉを生成し、選択されたクライアント機器へ、生成したＣＳＩ＿Ｉを送信する。また、ＡＤ内サーバＪも同様に、ＣＳＩ＿Ｊを生成してクライアント機器へ送信する。

【０４４０】

なお、ＡＤ内サーバＩ及びＪは、クライアント機器を選択する度に認証しても良いし、新たに生成したＣＳＩを送信する際に認証するとしても良い。

また、上記のように、１つのＡＤから新たに２つのＡＤを形成する他、ＡＤ＿Ｈから新たなＡＤを一つ形成し、基になったＡＤ＿Ｈと新たなＡＤとの２つに分割するとしても良い。

（２９）クライアント機器が電源を切ると、クライアント機器はＡＤ内サーバに登録されたまま、ＣＳＩは一旦削除されるとしても良い。

【０４４１】

この場合、クライアント機器がＡＤ内サーバに登録されると、ＡＤ内サーバはクライアント機器のＩＤを記憶し、ＣＳＩを送信する。

クライアント機器は、受け取ったＣＳＩを記憶すると、ＡＤ内機器としてコンテンツを利用できる。クライアント機器は、電源ＯＦＦの指示を受け付けると、ＣＳＩを削除し、電源をＯＦＦにする。この際、ＡＤ内サーバが記憶しているクライアント機器のＩＤは削除されない。

【０４４２】

再びクライアント機器の電源がＯＮになると、クライアント機器は、ＡＤ内サーバにＩＤを送信する。ＡＤ内サーバは、記憶しているＩＤに、受信したＩＤと一致するＩＤが有るか否かを判断し、一致するＩＤが有る場合、登録情報を更新せずに、クライアント機器にＣＳＩを再送信する。

なお、有線又は無線通信が遮断された場合も同様にＣＳＩを一旦消去し、通信が再度確立されると、ＩＤを送信し、ＣＳＩを再度取得するとしても良い。

（３０）本実施の形態では、ＣＳＩを用いて認証を行うとしたが、更に、以下の（ａ）～（ｃ）の認証を追加しても良い。

【０４４３】

（ａ）ＭＡＣアドレスやＩＰアドレス、またシステムで統一的に与えられたコードなどを用いてクライアント機器がＡＤ内サーバと同一の家庭内ＬＡＮに接続されていることを認証する。これにより、他人のクライアント機器を登録することが困難になる。

また、ＡＤ内サーバとクライアント機器とが無線で通信を行う場合、電波の届く範囲であることで認証しても良い。

【０４４４】

また、ＡＤ内サーバとクライアント機器とが通信可能な場合、ＡＤ内サーバからクライアント機器へ、認証用データを送信し、クライアント機器は、認証用データを受信すると、応答データをＡＤ内サーバへ送信する。ＡＤ内サーバは、認証用データを送信してから応答データを受信するまでの時間を計時し、計時した時間が、予め設定している　値以内であれば、同一宅内に設置されているものと認証するとしても良い。

【０４４５】

また、ＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）値を宅内のルータの数以内に設定し、宅外の機器とは通信できないようにしても良い。

また、同じ電源に接続されているか否かを判断することで、同一宅内に設置されているか否かを認証するとしても良い。

（ｂ）ＡＤ内サーバに予めパスワードを設定しておき、クライアント機器を登録する際、ユーザは前記パスワードをクライアント機器に手入力する。クライアント機器は入力されたパスワードを含む登録要求をＡＤ内サーバへ送信し、ＡＤ内サーバは、登録要求に含んで受信したパスワードが、予め設定されたパスワードと一致するか否かを判断する。

【０４４６】

また、パスワードは複数設定しても良く、例えば家族それぞれが自分のパスワードを設定するとしても良い。また、ユーザそれぞれを識別するＩＤとパスワードとを組み合わせるとしても良い。

（ｃ）上記（ｂ）におけるパスワードの代わりに、指紋や虹彩などのバイオメトリックス情報を使用しても良い。これにより、予め設定した本人だけがクライアント機器の登録を行うことが可能となる。

（３１）クライアント機器が保持している初期値は、以下（ａ）～（ｃ）の場合がある。

【０４４７】

（ａ）クライアント機器は、ＡＤ内サーバに登録していないことを示す、１個の初期値を保持している。当該ＡＤ内サーバに登録されると、初期値の使用が抑制される。

（ｂ）クライアント機器は、複数のＡＤ内サーバそれぞれに対応する複数の初期値を保持している。複数のＡＤ内サーバの何れかに登録する際、当該ＡＤ内サーバに対応する初期値を用いて認証し、登録されると、前記対応する初期値の使用を抑制する。また、他のＡＤ内サーバに登録されると、他のＡＤ内サーバに対応する初期値の使用を抑制する。

【０４４８】

なお、それぞれの初期値をグループの識別子に対応付けて識別しても良い。

（ｃ）クライアント機器は、複数のＡＤ内サーバの、何れにも登録していないことを示す初期値を保持している。何れかのＡＤ内サーバに登録すると、初期値の使用を抑制する。

（３２）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０４４９】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている
前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０４５０】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０４５１】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（３３）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

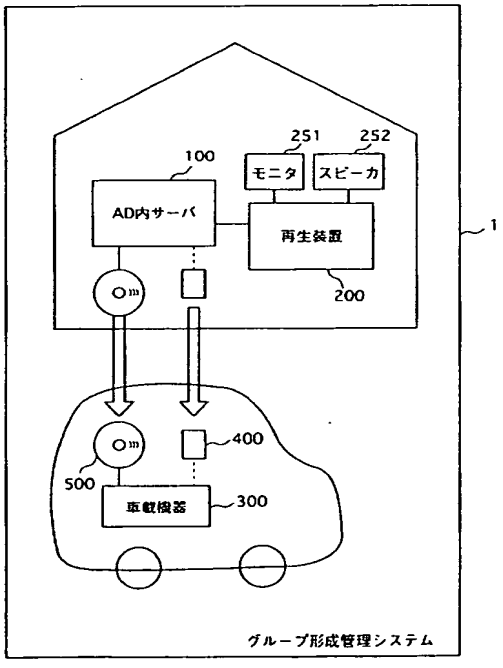
【産業上の利用可能性】
【０４５２】
複製コンテンツの数を規制したコンテンツの管理に利用できる。
【図面の簡単な説明】
【０４５３】
【図１】グループ形成管理システム１の全体の構成を示すブロック図である。
【図２】ＡＤ内サーバ１００の構成を示すブロック図である。
【図３】登録情報の構成を示す図である。
【図４】再生装置２００の構成を示すブロック図である。
【図５】車載機器３００の構成を示すブロック図である。
【図６】ＩＣカード４００の構成を示すブロック図である。
【図７】ＳＡＣ確立の処理を示すフローチャートである。図８に続く。
【図８】ＳＡＣ確立の処理を示すフローチャートである。図７の続き。
【図９】再生装置２００をＡＤ内サーバ１００に登録する際の動作を示すフローチャートである。
【図１０】車載機器３００を登録する際の動作を示すフローチャートである。
【図１１】車載機器３００を登録する際の動作を示すフローチャートである。
【図１２】コンテンツを配送する際の動作を示すフローチャートである。
【図１３】コンテンツを配送する際の動作の一部を示すフローチャートである。
【図１４】コンテンツをＤＶＤに記録する際の動作を示すフローチャートである。
【図１５】ＡＤ内サーバ１００から脱退する際の動作を示すフローチャートである。
【図１６】鍵配信システム１０００を示すブロック図である。
【図１７】コンテンツサーバ１００１を示すブロック図である。
【図１８】コンテンツ記憶部１０１１を示すブロック図である。
【図１９】管理情報記憶部１０１２を示すブロック図である。
【図２０】鍵情報記憶部１０３１が有する鍵情報テーブルＴ１００１のデータ構造を示す。
【図２１】配信鍵情報記憶部１０３２が有する配信鍵情報テーブルＴ１００２のデータ構造を示す。
【図２２】記録媒体１００２を示すブロック図である。
【図２３】利用鍵記憶部１１０２が有する配信コンテンツ鍵テーブルＴ１１０１のデータ構造を示す。
【図２４】再生装置１００３を示すブロック図である。
【図２５】再生装置１００４を示すブロック図である。
【図２６】コンテンツ鍵管理処理を示す流れ図である。図２７へ続く。
【図２７】コンテンツ鍵管理処理を示す流れ図である。図２８から続く。
【図２８】認証処理を示す流れ図である。
【図２９】時間管理処理を示す流れ図である。
【図３０】再生装置１００４における再生時の動作を示す流れ図である。
【図３１】再生装置１００３における再生時の動作を示す流れ図である。
【図３２】コンテンツサーバ１００１にて記録媒体１００２の利用時の動作を示す流れ図である。
【図３３】コンテンツサーバ１００１における再生時の動作を示す流れ図である。
【図３４】鍵確認処理を示す流れ図である。
【図３５】コンテンツ鍵の事前配信時の動作を示す流れ図である。
【図３６】コンテンツ複製管理システム２０００の構成を示すブロック図である。
【図３７】ホームサーバ２００１の構成を示すブロック図である。
【図３８】複製制限情報管理部２１０２が保持する情報を示す。
【図３９】再生装置２００２の構成を示すブロック図である。
【図４０】再生装置２００３とＩＣ内蔵可搬型記憶媒体２００４との構成を示すブロック

図である。
【図４１】再生装置２００６の構成を示すブロック図である。
【図４２】コンテンツ複製元決定処理を示すフローチャートである。
【図４３】配信装置と要求装置との間で行われる相互の機器認証及び鍵共有の動作を示すフローチャートである。
【図４４】配信装置と要求装置との間で行われる相互の機器認証及び鍵共有の動作を示すフローチャートである。
【図４５】コンテンツの複製処理を示す図である。
【図４６】複製制限管理情報譲渡処理を示すフローチャートである。
【図４７】使用期限の定まったコンテンツを管理する使用期限管理処理を示す。
【図４８】コンテンツの複製予約実行処理を示す図である。
【図４９】コンテンツ返却処理を示すフローチャートである。
【図５０】複数のクライアント機器を、代表の機器がＡＤ内サーバに登録する場合の構成を示すブロック図である。
【図５１】複数のグループから一つのグループを形成する場合の概念を示す図である。
【図５２】一つのグループを分割して複数のグループを形成する場合の概念を示す図である。
【符号の説明】
【０４５４】

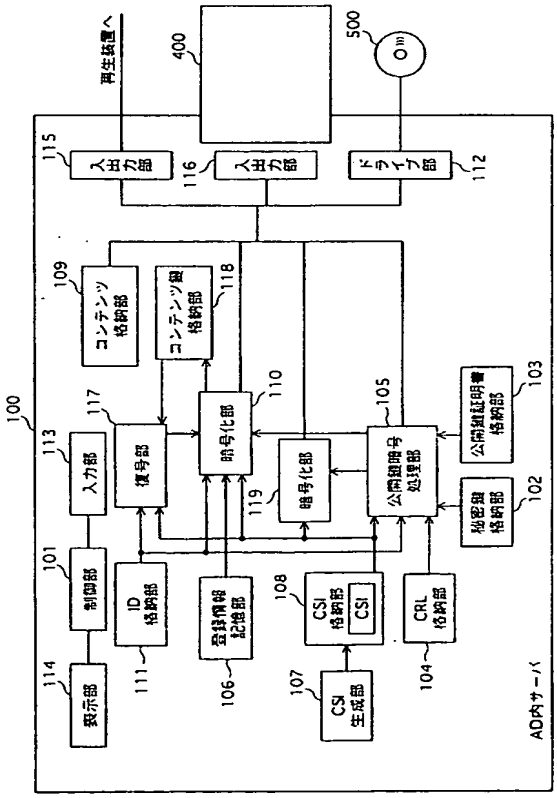
１	グループ形成管理システム
１０００	鍵配信システム
１００１	コンテンツサーバ
Ｔ１００１	鍵情報テーブル
１００２	記録媒体
Ｔ１００２	配信鍵情報テーブル
１００３	再生装置
１００４	再生装置
１００５	再生装置
１００６	放送局
１００７	ＧＷ
１０１１	コンテンツ記憶部
１０１２	管理情報記憶部
１０１３	利用鍵記憶部
１０１４	受信部
１０１５	コンテンツ取得部
１０１６	入力部
１０１７	再生部
１０１８	利用鍵監視部
１０１９	利用鍵確認部
１０２０	利用鍵事前配信部
１０２１	コンテンツ鍵制御部
１０２２	認証部
１０２３	時間管理部
１０２４	入出力部
１０２５	通信部
１０２６	時計部
１０３１	鍵情報記憶部
１０３２	配信鍵情報記憶部
１１０１	コンテンツ記憶部
Ｔ１１０１	配信コンテンツ鍵テーブル

1102	利用鍵記憶部
1103	認証部
1104	入出力部
1201	入力部
1202	再生部
1203	利用鍵確認部
1204	入出力部
1205	通信部
1206	時計部
1301	コンテンツ記憶部
1302	利用鍵記憶部
1303	入力部
1304	再生部
1305	利用鍵監視部
1306	認証部
1307	通信部
1310	時計部
1311	時間管理部

【図１】



【図２】



【図３】

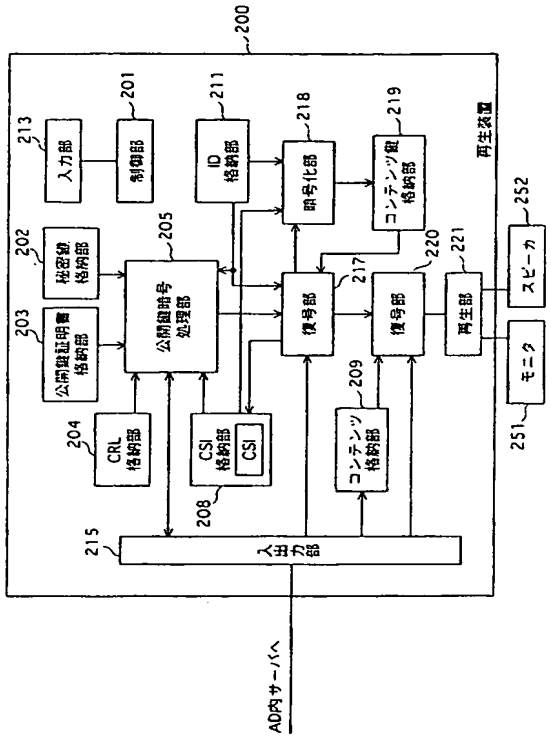
(a)

登録情報	
機器ID	
最大	2
登録台数	0
残数	2
ICカードID	ID_4

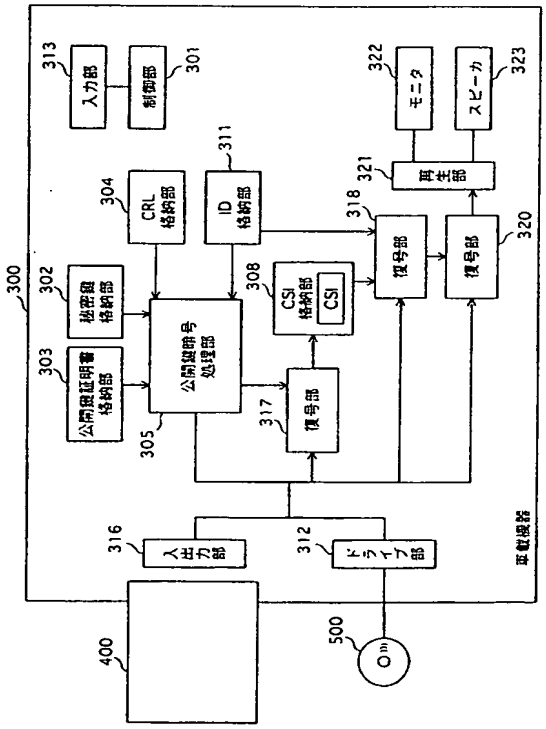
(b)

登録情報	
機器ID	ID_2
	ID_3
最大	2
登録台数	2
残数	0
ICカードID	ID_4

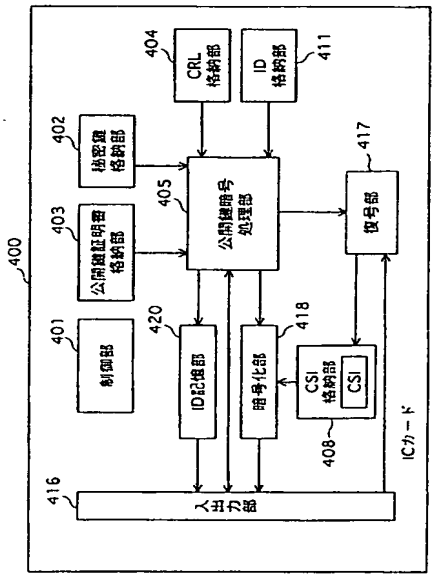
【図４】



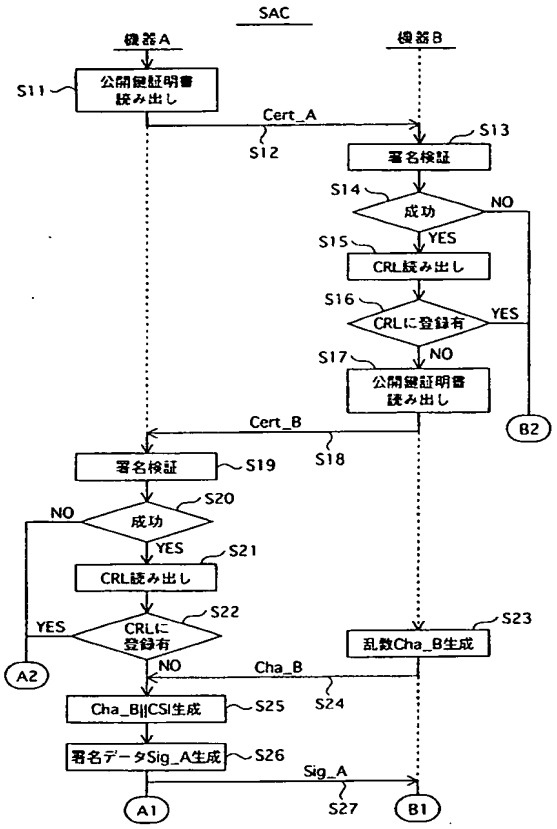
【図５】



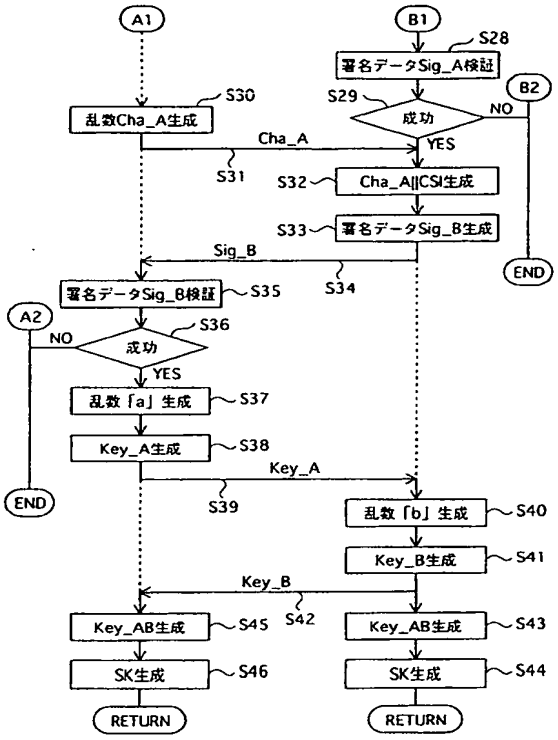
【図６】



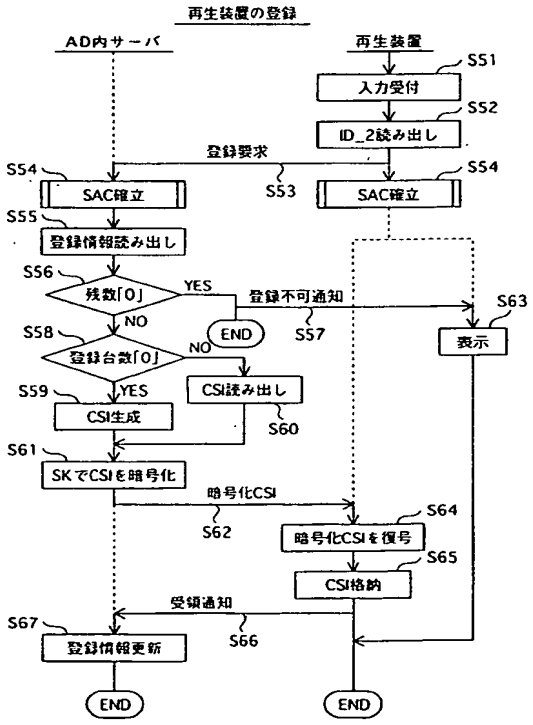
【図７】


SAC
機器A
機器B
公開鍵証明書読み出し
S11
Cert_A
S12
署名検証
S13
成功
S14
NO
YES
CRL読み出し
S15
CRLに登録有
S16
YES
NO
公開鍵証明書読み出し
S17
B2
Cert_B
S18
署名検証
S19
成功
S20
NO
YES
CRL読み出し
S21
CRLに登録有
S22
YES
NO
A2
乱数Cha_B生成
S23
Cha_B
S24
Cha_B||CSI生成
S25
署名データSig_A生成
S26
Sig_A
S27
A1
B1

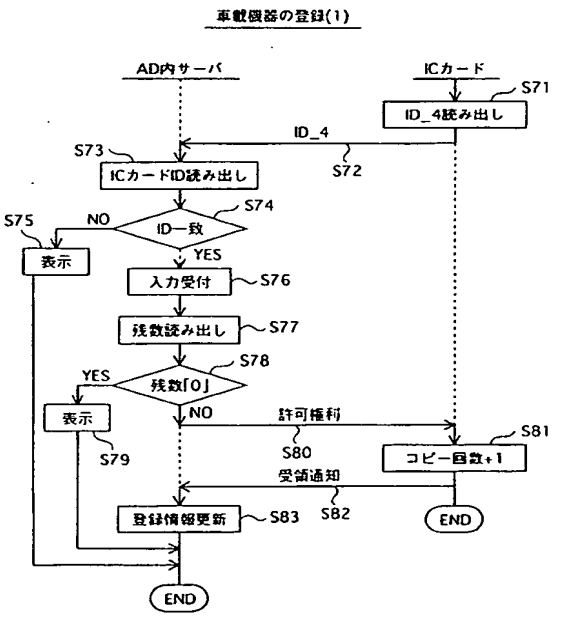
【図８】


A1
B1
署名データSig_A検証
S28
乱数Cha_A生成
S30
成功
S29
NO
B2
YES
Cha_A
S31
S32
Cha_A||CSI生成
S33
署名データSig_B生成
Sig_B
S34
END
署名データSig_B検証
S35
A2
NO
成功
S36
YES
乱数「a」生成
S37
Key_A生成
S38
Key_A
S39
END
乱数「b」生成
S40
Key_B生成
S41
Key_B
S42
Key_AB生成
S45
Key_AB生成
S43
SK生成
S46
SK生成
S44
RETURN
RETURN

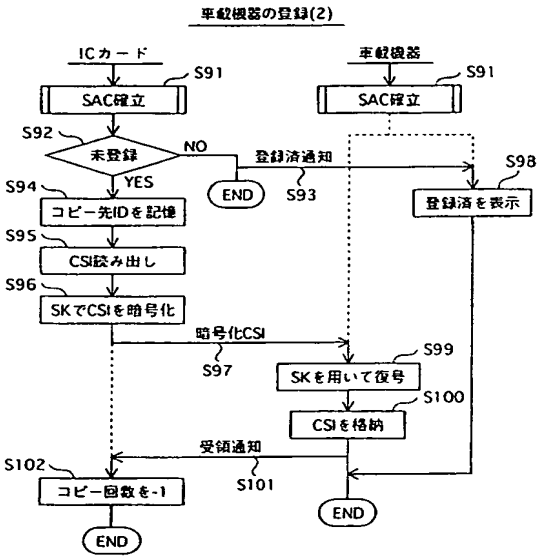
【図９】


再生装置の登録
AD内サーバ
再生装置
入力受付
S51
ID_2読み出し
S52
登録要求
S53
S54
SAC確立
SAC確立
S54
登録情報読み出し
S55
残数「0」
S56
YES
登録不可通知
S63
NO
END
S57
表示
登録台数「0」
S58
NO
CSI読み出し
YES
S59
CSI生成
S60
SKでCSIを暗号化
S61
暗号化CSI
S62
暗号化CSIを復号
S64
CSI格納
S65
受領通知
S66
登録情報更新
S67
END
END

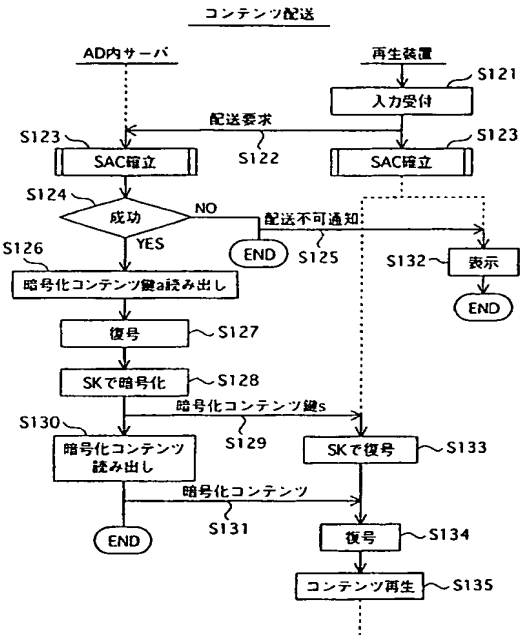
【図１０】


車載機器の登録(1)
AD内サーバ
ICカード
ID_4読み出し
S71
ID_4
S72
ICカードID読み出し
S73
ID一致
S74
S75
NO
YES
表示
入力受付
S76
残数読み出し
S77
残数「0」
S78
YES
NO
表示
S79
許可権利
S80
コピー回数+1
S81
受領通知
S82
登録情報更新
S83
END
END

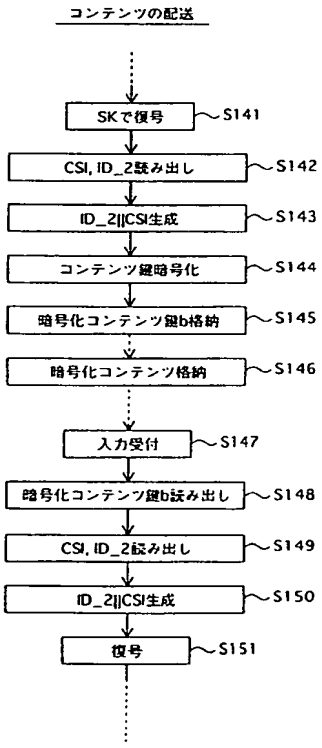
【図１１】



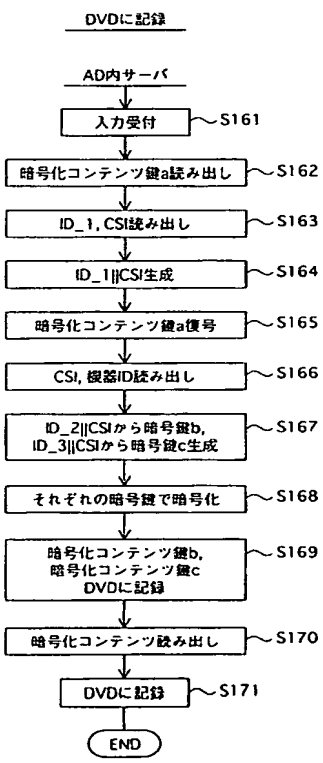
【図１２】



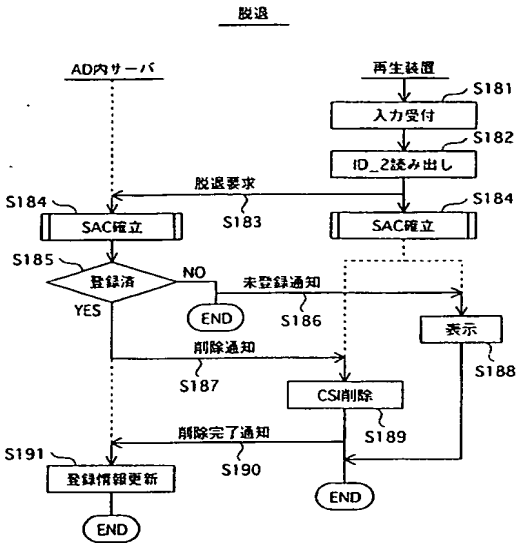
【図１３】



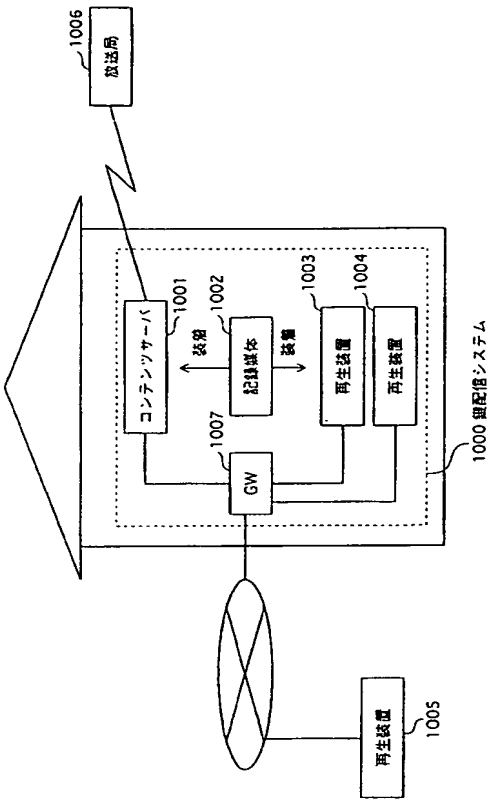
【図１４】



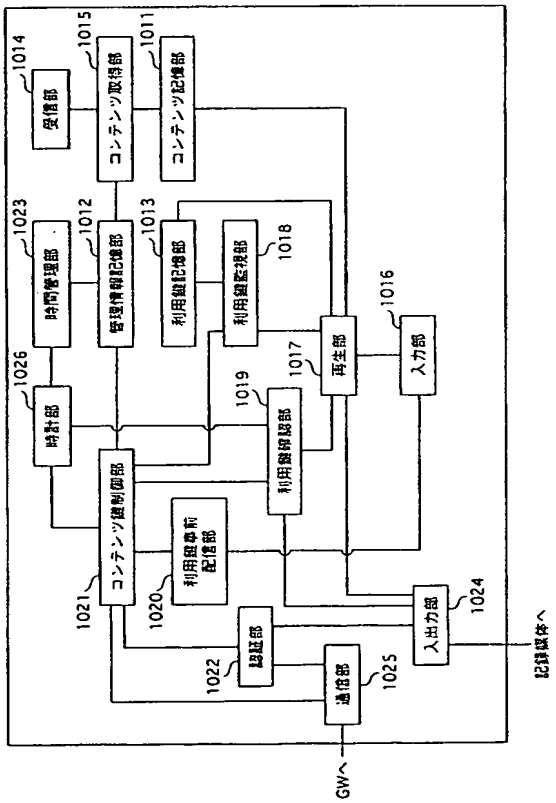
【図１５】



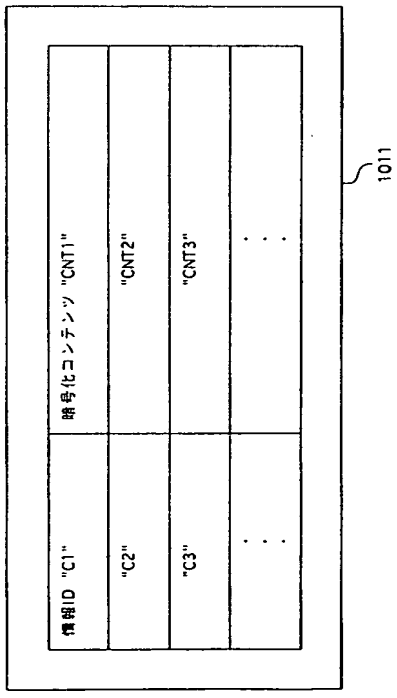
【図１６】



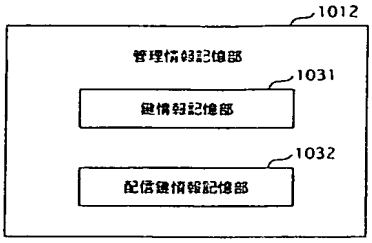
【図１７】



【図１８】



【図１９】



【図２０】

T1001

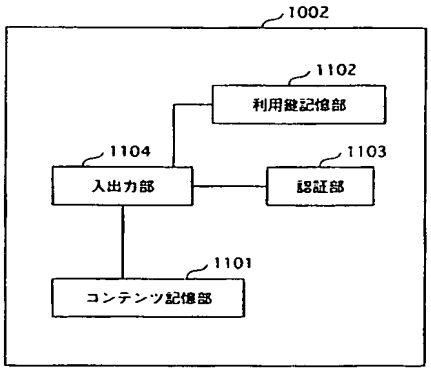
コンテンツ鍵ID	コンテンツ鍵	対応情報ID	総数	残数	制限時間
1	CK1	C1	5	4	24時間
2	CK2	C2	5	3	24時間
3	CK3	C3	5	5	24時間
・・・	・・・	・・・	・・・	・・・	・・・

【図２１】

T1002

配信コンテンツ鍵ID	利用期限
1	2003/7/10 19：00
2	2003/7/10 21：30
・	・
・	・
・	・

【図２２】

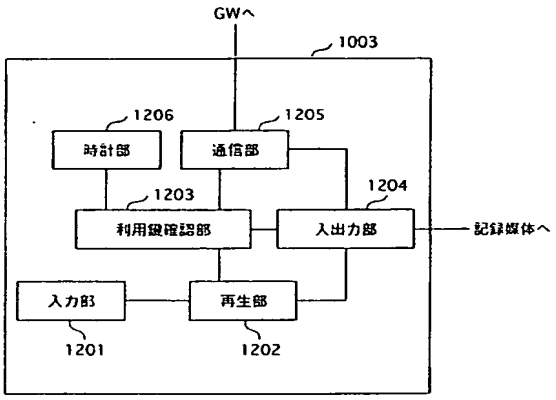


【図２３】

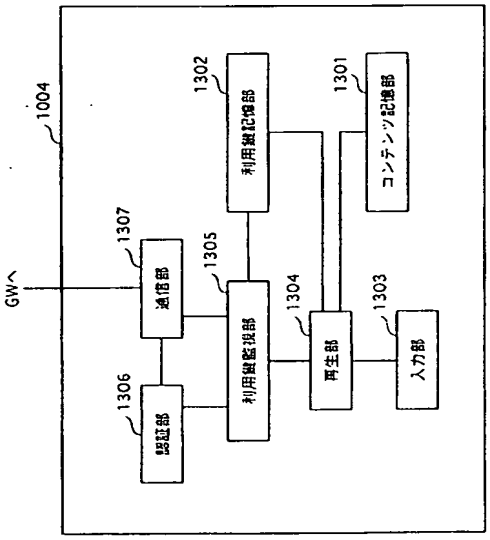
T1101

コンテンツ鍵ID	コンテンツ鍵	対応情報ID	利用期限
1	CK1	C1	2003/7/10 19:00
2	CK2	C2	2003/7/10 21:30
・・・	・・・	・・・	・・・

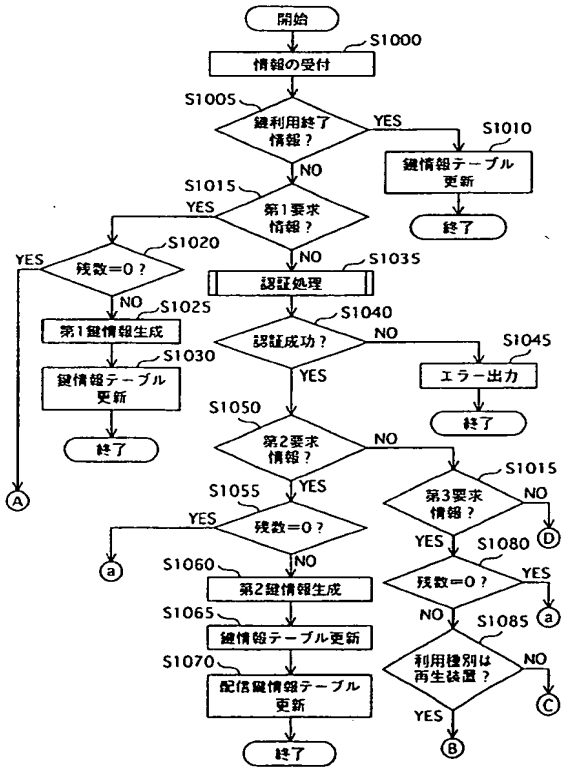
【図２４】



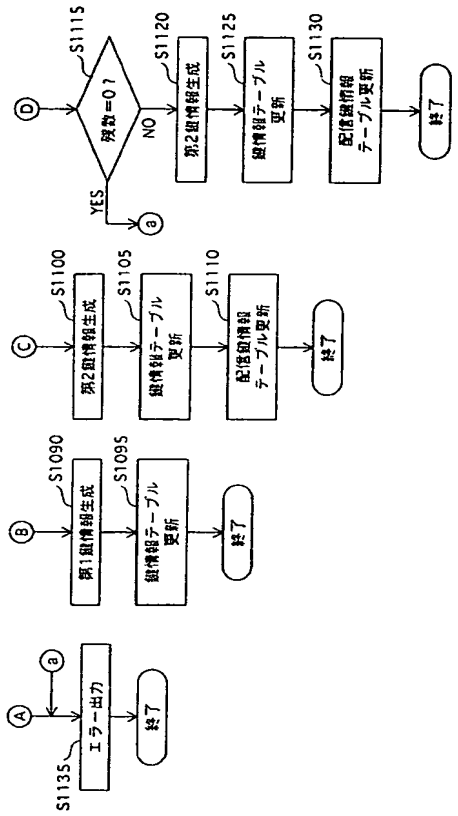
【図２５】



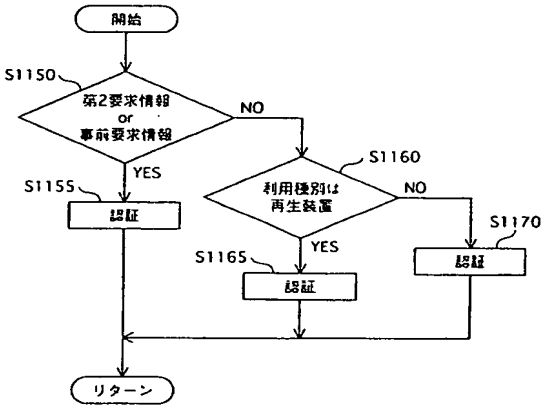
【図２６】



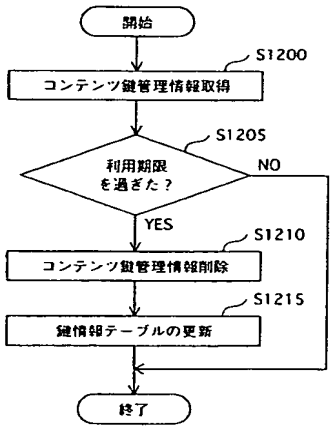
【図２７】



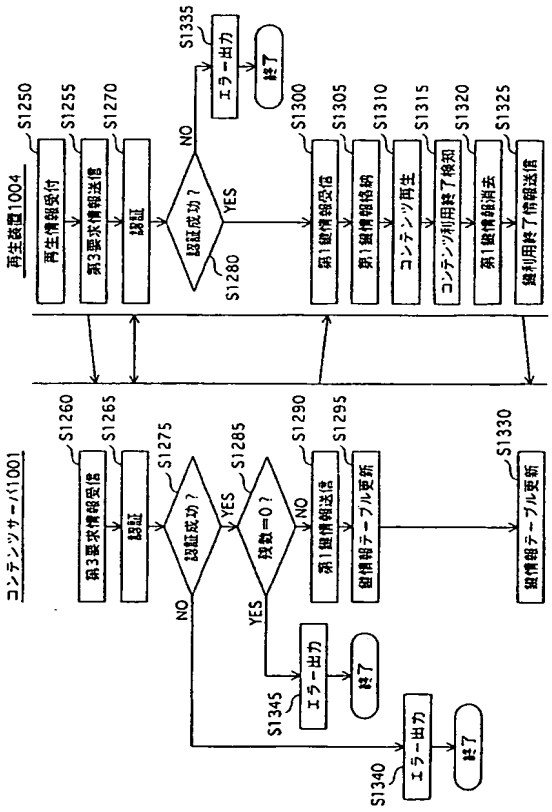
【図２８】



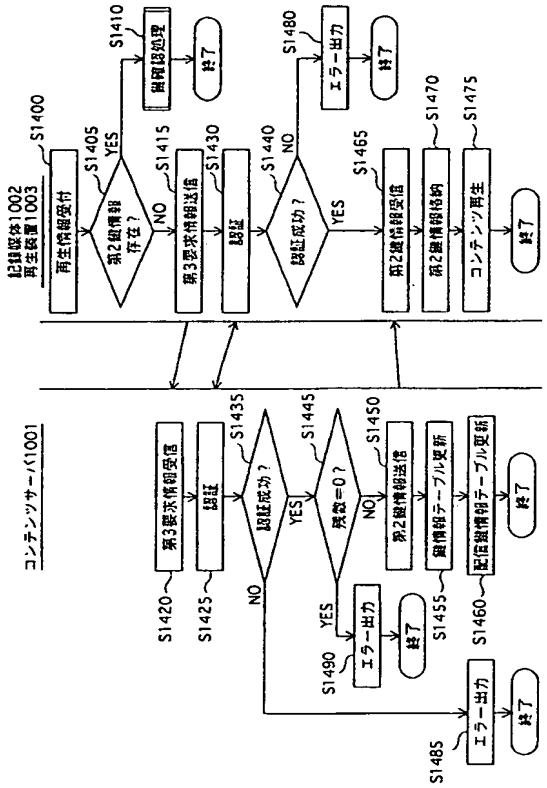
【図２９】



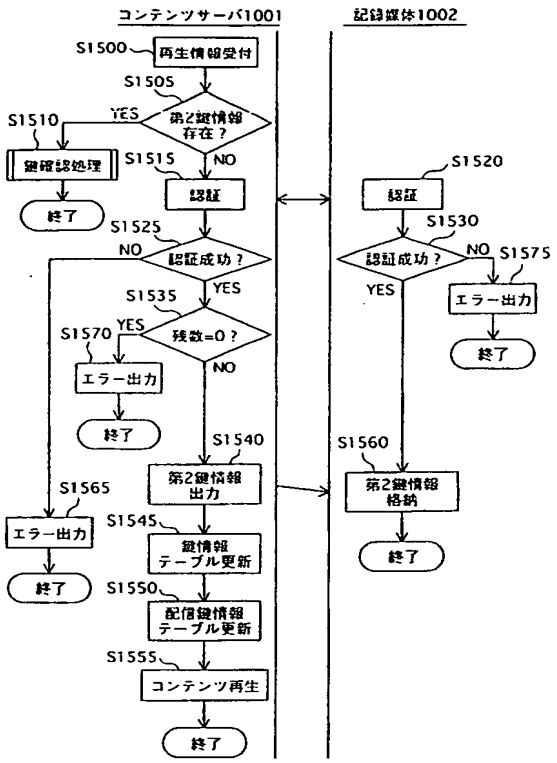
【図３０】



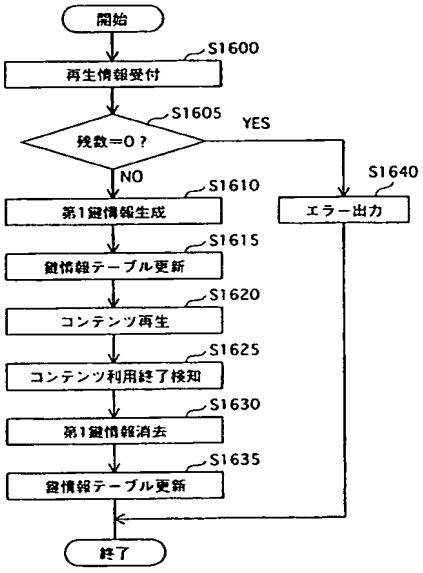
【図３１】



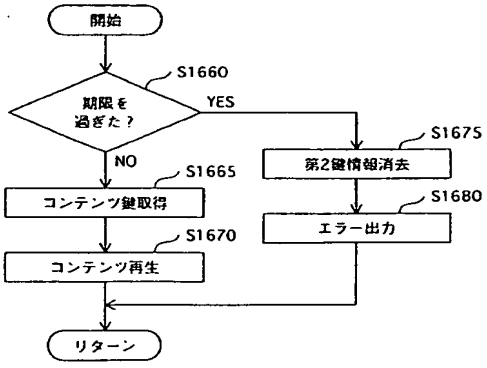
【図３２】



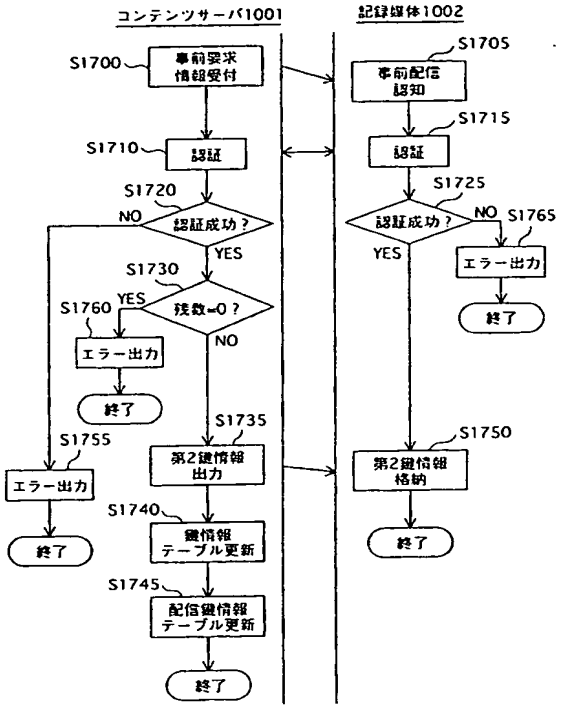
【図３３】



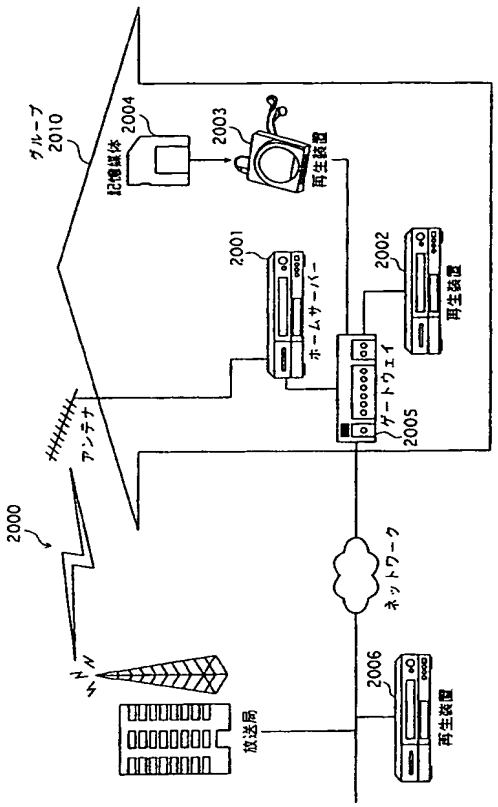
【図３４】



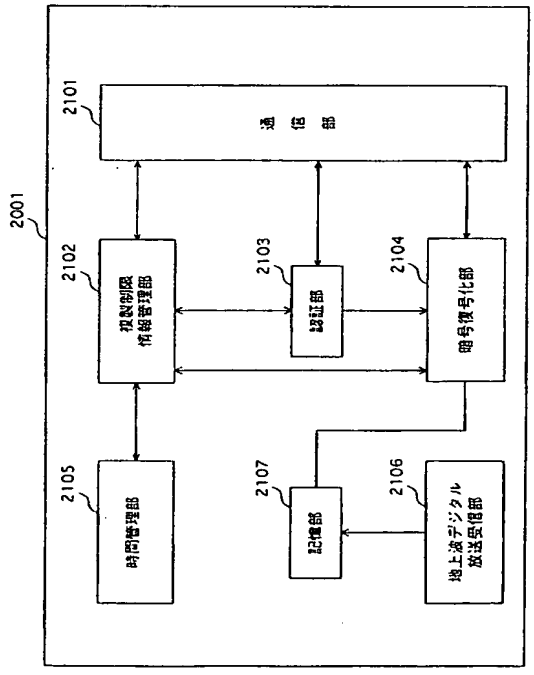
【図３５】



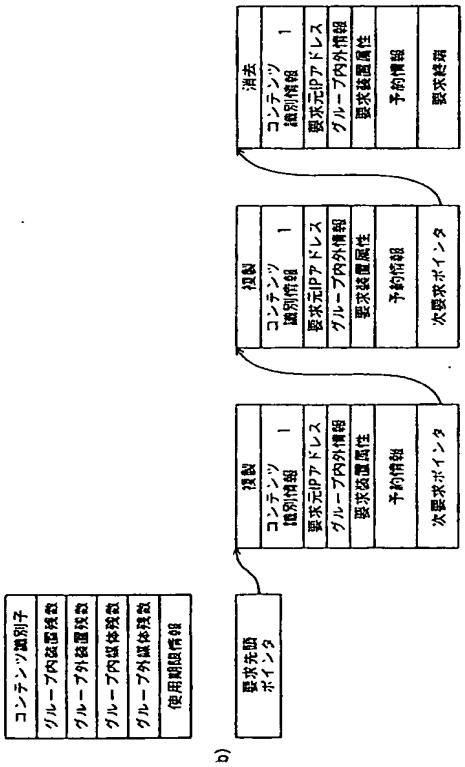
【図３６】



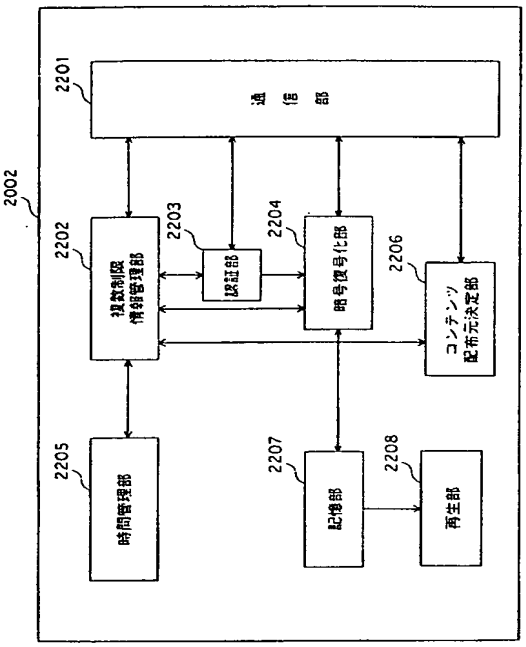
【図３７】



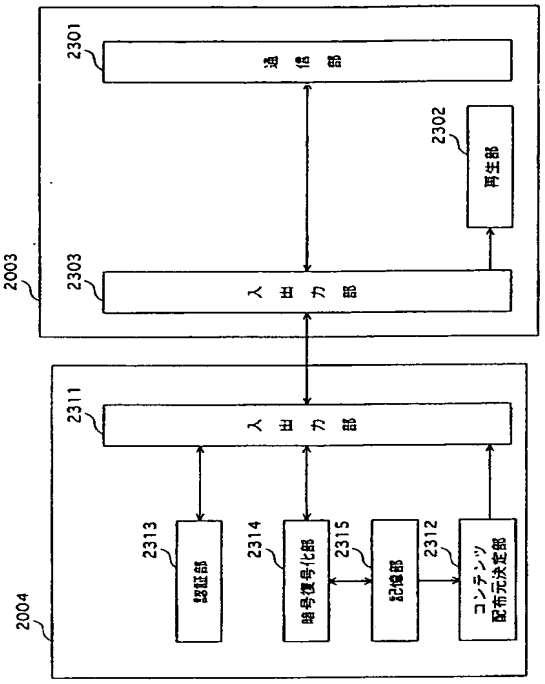
【図３８】



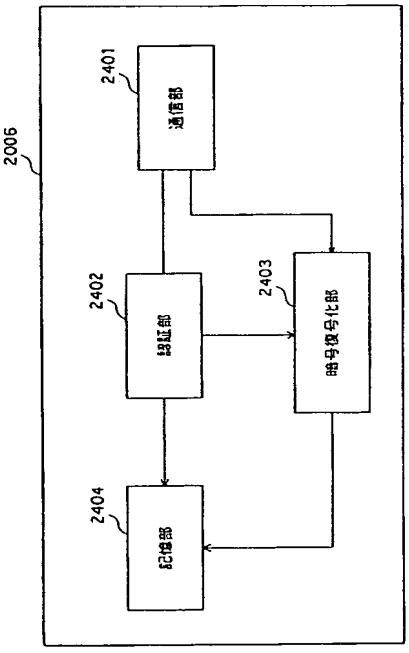
【図３９】



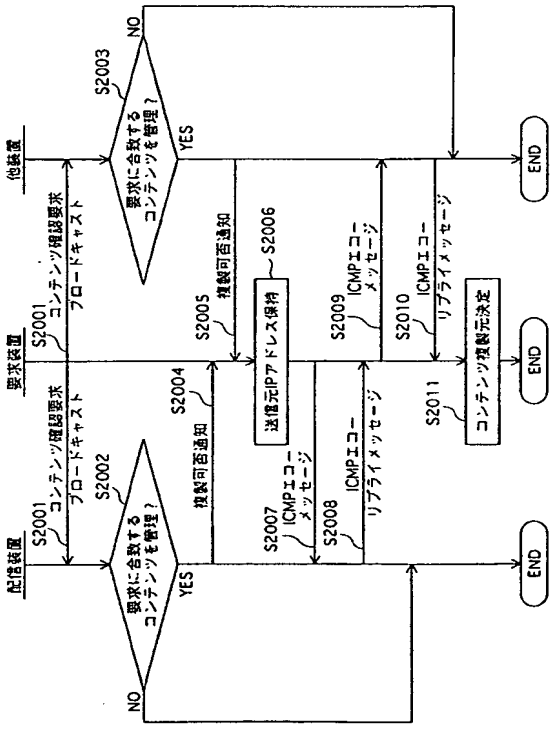
【図４０】



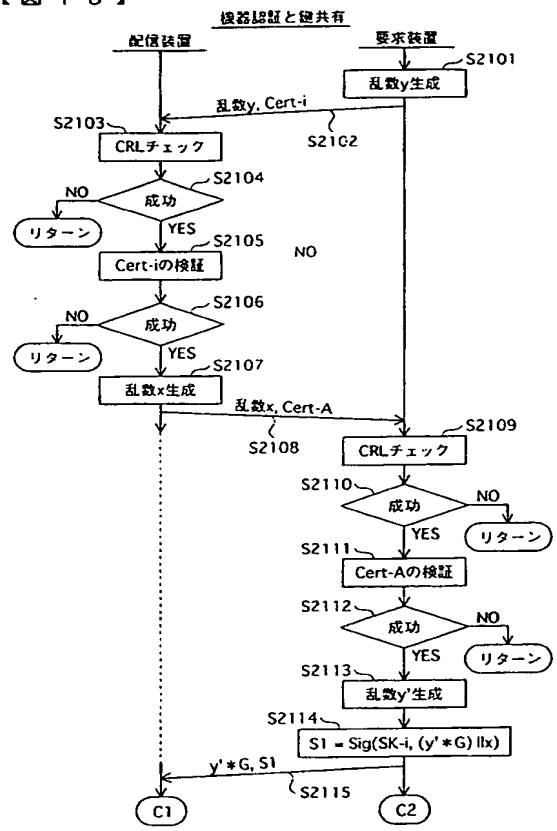
【図４１】



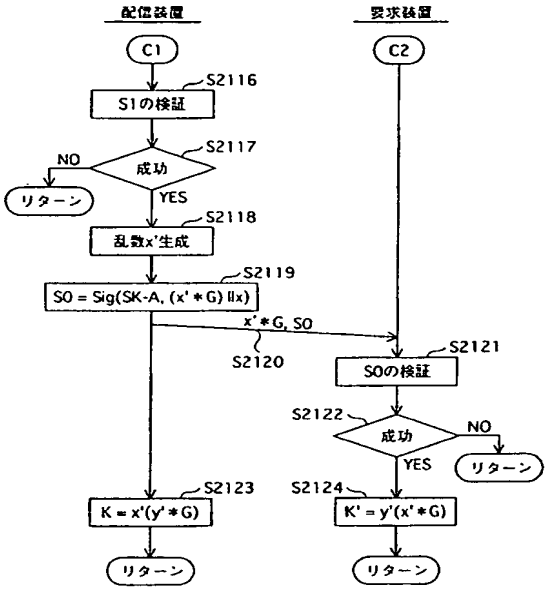
【図４２】



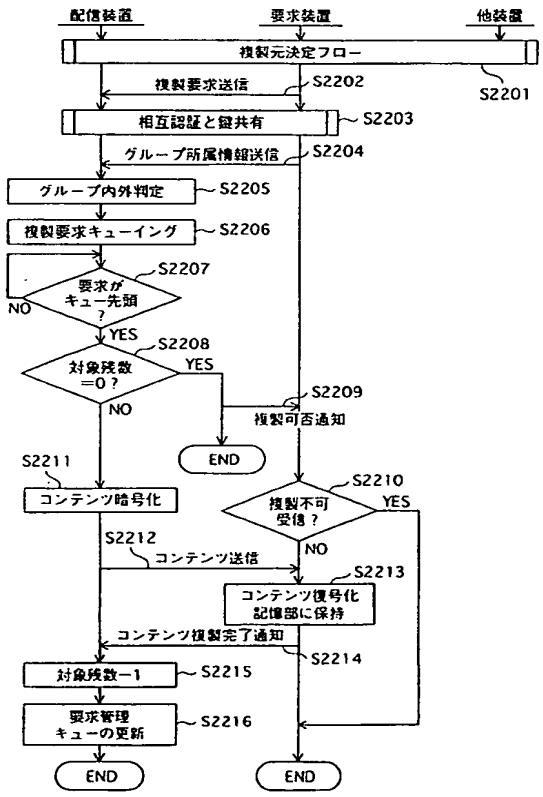
【図４３】



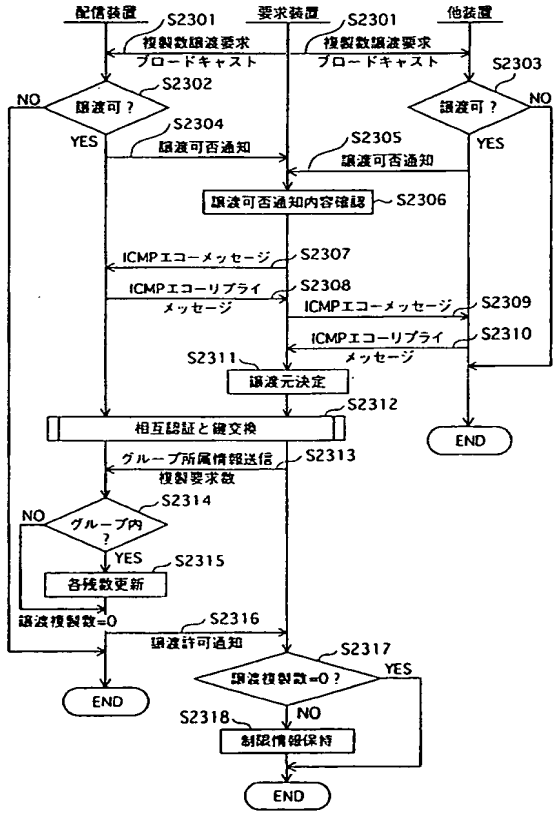
【図４４】



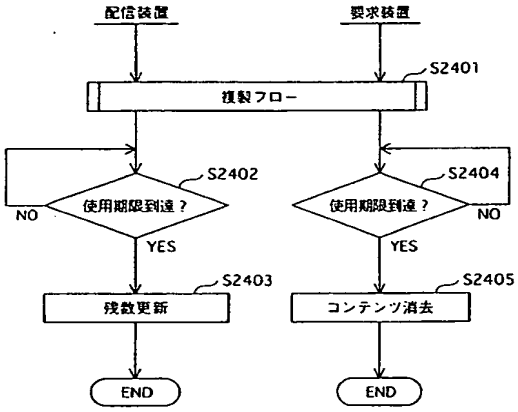
【図４５】



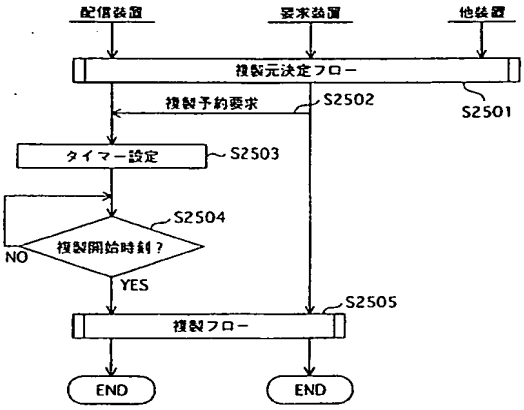
【図４６】



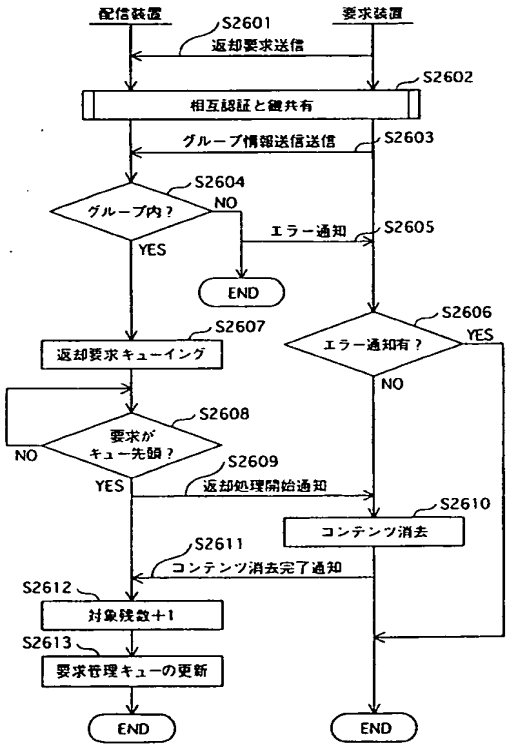
【図４７】



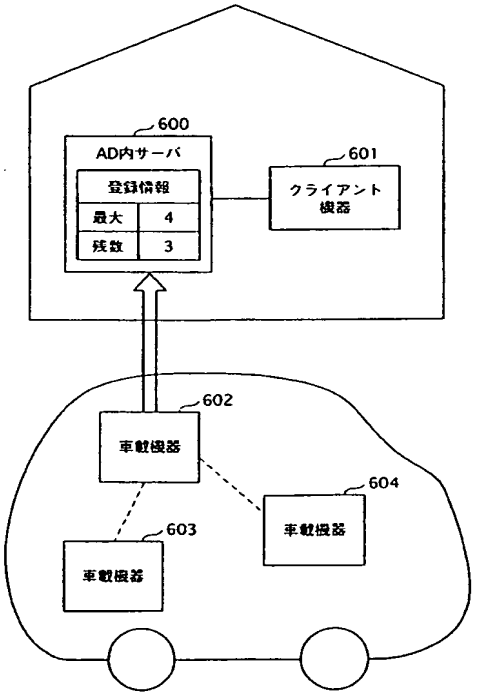
【図４８】



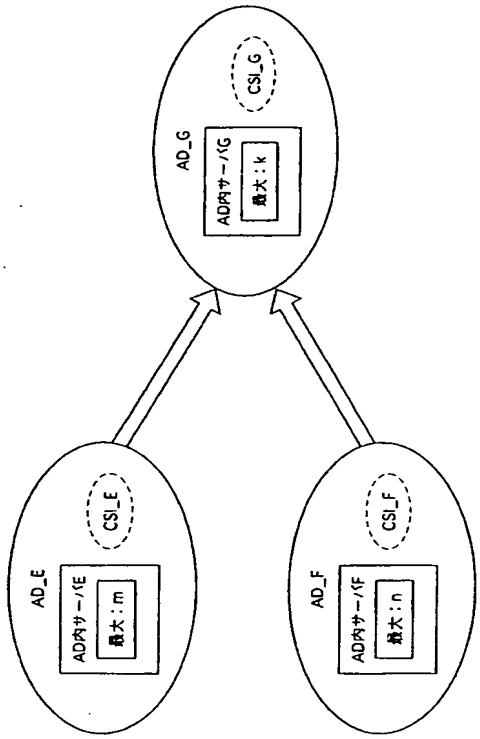
【図４９】



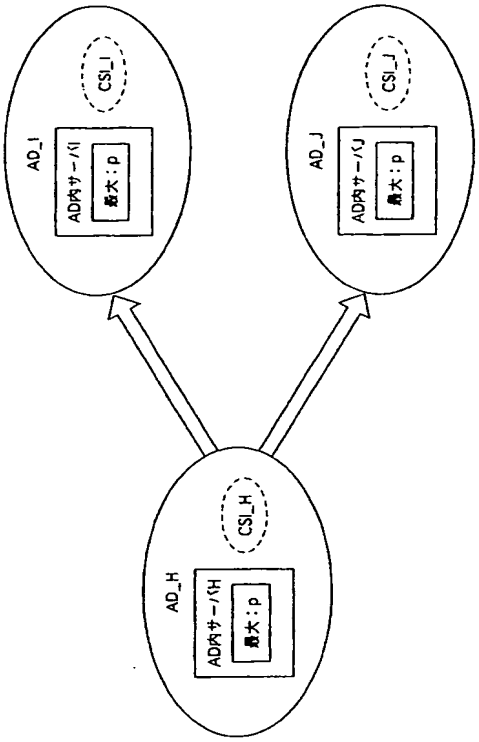
【図５０】



【図５１】


AD_G
CSI_G
AD内サーバG
最大：k
AD_E
CSI_E
AD内サーバE
最大：m
AD_F
CSI_F
AD内サーバF
最大：n

【図５２】


AD_I
CSI_I
AD内サーバI
最大：p
AD_J
CSI_J
AD内サーバJ
最大：p
AD_H
CSI_H
AD内サーバH
最大：p

フロントページの続き

(72)発明者 松崎 なつめ
大阪府門真市大字門真１００６番地 松下電器産業株式会社内
(72)発明者 阿部 敏久
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

Ｆターム(参考) 5J104 EA17